646–3347 or e-mail address: *FEMA-Information-Collections@dhs.gov*.

Dated: December 18, 2008.

Samuel C. Smith,

Acting Director, Records Management Division, Office of Management, Federal Emergency Management Agency, Department of Homeland Security.

[FR Doc. E8–30721 Filed 12–23–08; 8:45 am]

BILLING CODE 9110–11–P

DEPARTMENT OF HOMELAND SECURITY

Federal Emergency Management Agency

[Docket ID FEMA–2008–0017]

Voluntary Private Sector Accreditation and Certification Preparedness Program

AGENCY: Federal Emergency Management Agency, DHS.

ACTION: Notice; request for recommendations.

SUMMARY: In the ''Implementing the Recommendations of the 9/11 Commission Act of 2007'' (the 9/11 Act), Congress authorized the Department of Homeland Security (DHS) to establish a voluntary private sector preparedness accreditation and certification program. This program, now known as ''PS-Prep,'' will assess whether a private sector entity complies with one or more voluntary preparedness standards adopted by DHS, through a system of accreditation and certification set up by DHS in close coordination with the private sector.

PS-Prep will raise the level of private sector preparedness through a number of means, including (i) Establishing a system for DHS to adopt private sector preparedness standards; (ii) encouraging creation of those standards; (iii) developing a method for a private sector entity to obtain a certification of conformity with a particular DHS-adopted private sector standard, and encouraging such certification; and (iv) making preparedness standards adopted by DHS more widely available.

This Notice discusses essential elements of the program, describes the consultation that has taken place and will take place with the private sector, and seeks additional recommendations in a number of areas, including the private sector preparedness standards that DHS should adopt, both initially and over time.

DATES: *Comment period:* Anyone may submit comments on this guidance at any time, and comments will be considered as they are received. We would appreciate any recommendations for adoption of currently-existing private sector preparedness standards by January 23, 2009, though, as made clear below, we will accept submissions of private sector preparedness standards for adoption as well as comments on this notice at any time.

Public Meetings: DHS intends to hold two public meetings in Washington, DC to provide a forum for public comment on the subject of private sector preparedness standards, one in January and another in February, 2009. Meeting details and registration information will be published in the **Federal Register** and posted at *http://www.fema.gov/privatesectorpreparedness.*

ADDRESSES: You may submit comments, identified by Docket ID FEMA–2008–0017, by one of the following methods:

Federal eRulemaking Portal: http://www.regulations.gov. Follow the instructions for submitting comments. (All government requests for comments—even if, as in this case, they are not for regulatory purposes—are sent to this portal.)

E-mail: FEMA-POLICY@dhs.gov. Include Docket ID FEMA–2008–0017 in the subject line of the message.

Fax: 866–466–5370.

Mail/Hand Delivery/Courier: Office of Chief Counsel, Federal Emergency Management Agency, 500 C Street, SW., Room 845, Washington, DC 20472.

Instructions: All submissions received must include the agency name and docket number (if available). Regardless of the method used for submitting comments or material, all submissions will be posted, without change, to the Federal eRulemaking Portal at *http://www.regulations.gov,* and will include any personal information you provide. Therefore, submitting this information makes it public. You may wish to read the Privacy Act notice that is available on the Privacy and Use Notice link on the Administration Navigation Bar of *http://www.regulations.gov*.

Docket: For access to the docket to read background documents or comments received, go to the Federal eRulemaking Portal at *http://www.regulations.gov*. Submitted comments may also be inspected at FEMA, Office of Chief Counsel, 500 C Street, SW., Room 840, Washington, DC 20472.

FOR FURTHER INFORMATION CONTACT: Mr. Don Grant, Incident Management Systems Director, National Preparedness Directorate, FEMA, 500 C Street SW., Washington, DC 20472. Phone: (202) 646–8243 or e-mail: *Donald.Grant@dhs.gov*.

SUPPLEMENTARY INFORMATION: This supplementary information section is organized as follows:

Table of Contents

I. Background

A. Preparedness in the Wake of 9/11

Private-sector preparedness is not a luxury; it is a cost of doing business in the post- 9/11 world. It is ignored at a tremendous potential cost in lives, money, and national security.

This conclusion was reached by the National Commission on Terrorist Attacks Upon the United States—the 9/11 Commission—in making a specific finding about private sector preparedness. During the course of its inquiry, the Commission found that the private sector was not prepared for the aftermath of the 9/11 attacks, and that, despite 9/11, the private sector remained largely unprepared at the time of its final report. The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks Upon the United States at 398 (2004) (9/11 Commission Report). The 9/11 Commission's central recommendation in this area was that the Department of Homeland Security (DHS) promote private sector preparedness standards that establish a common set of criteria and terminology for preparedness, disaster management, emergency

management, and business continuity programs.[1] This recommendation was the genesis of the Voluntary Private Sector Preparedness Accreditation and Certification (PS-Prep) program.

It is well known that approximately 85% of that infrastructure which we consider to be ''critical'' is owned and operated by the private sector. Critical infrastructure and key resources, or CIKR, comprises systems and assets, whether physical or virtual, so vital to the United States that their incapacitation or destruction would have a debilitating impact on national security, national economic security, public health or safety, or any combination of those matters. Terrorist attacks on our CIKR as well as other manmade or natural disasters could significantly disrupt the functioning of government and business alike, and produce cascading effects far beyond the affected CIKR and physical location of the incident.

Since one of DHS's core functions is encouraging preparedness and protection of critical infrastructure, Congress gave DHS a range of specialized tools to carry out its private sector mission. Two of the most prominent of these tools are authorized in the Homeland Security Act: the Supporting Anti-terrorism by Fostering Effective Technologies Act of 2002 (the SAFETY Act),[2] implemented through the department's SAFETY Act program (6 CFR Part 25), and the Critical Infrastructure Information Act of 2002, implemented through the department's Protected Critical Infrastructure Information, or PCII, program (6 CFR Part 29). The SAFETY Act authorizes certain liability mitigation measures for providers of qualified anti-terrorism technologies, if those technologies are alleged to have failed in the course of a terrorist attack. The PCII program allows entities to create assessments of the security of their critical infrastructure and share such assessments with DHS without the risk that such information, once shared, can be used against it in court or be publicly disclosed.

[1] The Commission specifically advocated that DHS promote a specific standard: The American National Standards Institute's (ANSI) standard for private preparedness. That standard is discussed below. The Commission also recommended that conformity with that standard define the standard of care owed by a company and its employees for legal purposes, and that insurance and credit-rating services look closely at a company's conformity with the ANSI standard in assessing its insurability and creditworthiness.

[2] Subtitle G of Title VIII of the Homeland Security Act of 2002, Public Law 107–296 (Nov. 25, 2002); 6 U.S.C. 441–444.

In the 9/11 Act, Congress authorized another tool for DHS to work with the private sector—PS-Prep—through which private sector entities can obtain certification of conformity with one or more voluntary preparedness standards adopted by DHS. Each of these programs has a common thread: that it is not DHS that will regulate preparedness or security in most corners of the private sector, but it is the private sector itself—with tools provided in part by DHS—that should take on that responsibility. In creating these programs, Congress recognized that achieving preparedness in the private sector is often more quickly and efficiently accomplished through incentives and certification processes made available to the to the private sector—since the private sector has greater resources and is generally more nimble than the Federal government—than through Federal regulatory mandates. PS-Prep will work with these other programs to leverage the powerful private sector tools DHS has been authorized to use.

B. Purpose and Structure of the Program

Simply stated, the purpose of PS-Prep is to widely encourage private sector preparedness. The program will do so by providing a mechanism for a private sector entity—a company, facility, not-for-profit corporation, hospital, stadium, university, etc.—to receive a certification from an accredited third party that it is in conformity with one or more private sector preparedness standards adopted by DHS.

Seeking certification will be completely voluntary: no private sector entity is required by DHS to seek or obtain a PS-Prep certification. For the reasons cited by the 9/11 Commission and discussed throughout this notice, however, DHS encourages all private sector entities to seriously consider seeking certification on appropriate standards adopted by DHS, once those standards become available. DHS also encourages private sector entities, including consensus standard development organizations and others, to develop preparedness standards that, if appropriate, may be adopted by DHS and become part of PS-Prep.

In order to accomplish its purpose, PS-Prep has three separate but interrelated components: adoption, accreditation, and certification.

- ''Adoption'' is DHS's selection of appropriate private sector preparedness standards for the program. Given DHS's goal of broadly encouraging private sector preparedness, we have developed a process, described below, that allows a wide variety of standards to be considered and adopted.
- ''Accreditation'' is a process managed by a DHS-selected non-governmental entity to confirm that a third party is qualified to certify that a private sector entity complies with a preparedness standard adopted by DHS. Third parties are ''accredited'' to provide certifications, and may be accredited on one, some, or all of the DHS-adopted standards.
- ''Certification'' is the process by which an accredited third party determines that a private sector entity is, in fact, in conformity with one of the private sector preparedness standards adopted by DHS.

II. Establishment of PS-Prep

A. Statutory Authorization

President George W. Bush signed the 9/11 Act into law on August 3, 2007. Section 901 of the 9/11 Act adds a new section 524 to the Homeland Security Act, codified at 6 U.S.C.321m, which requires the Secretary of Homeland Security to, among other things:

> develop and promote a program to certify the preparedness of private sector entities that voluntarily choose to seek certification under the program; and implement the program through an[] entity * * * which shall accredit third parties to carry out the certification process under this section.

This program is the PS-Prep program described in this notice.

B. The Designated Officer

In establishing and implementing the PS-Prep program, the Secretary of Homeland Security acts through a designated officer, who may be one of the following departmental officials: (i) The Administrator of the Federal Emergency Management Agency (FEMA); (ii) the Assistant Secretary for Infrastructure Protection; or (iii) the Under Secretary for Science and Technology. 6 U.S.C. 321m(a)(2). On August 31, 2007, the Secretary named the Administrator of FEMA as the designated officer.

C. The PS-Prep Coordinating Council

The designated officer is statutorily required to coordinate with the two other departmental officials named above—the Assistant Secretary for Infrastructure Protection and the Under Secretary for Science and Technology—as well as with the Special Assistant to the Secretary (now Assistant Secretary) for the Private Sector, in carrying out the program. 6 U.S.C. 321m(a)(3). This coordination takes place through the PS-Prep Coordinating Council (the PSPCC), which is described below. Other permanent members of the PSPCC include the DHS General Counsel and

the Assistant Secretary for Policy. The PSPCC will, in consultation with the private sector, adopt the preparedness standards to be certified through PS-Prep as described in this notice.

D. Coordination With the Private Sector and Other Non-DHS Entities

Even before the 9/11 Act became law, DHS encouraged private-sector owners of critical infrastructure to consider, develop and employ sector-specific preparedness best practices. DHS did so through communication with the Sector Coordinating Councils for the now eighteen critical infrastructure/key resources (CIKR) sectors, organizations that coordinate or facilitate the development of private sector preparedness standards, and other private sector parties. The private sector—which is responsible for roughly 85% of the critical infrastructure of the nation—has made substantial strides in this area, and through its and DHS's work, the private sector has become more prepared for disasters.

Since the 9/11 Act's enactment, DHS has continued this engagement, focusing specifically on the development and administration of PS-Prep. Work has already been done with private sector entities and their representatives, including representatives of organizations that coordinate the development and use of voluntary consensus standards and others.

This notice is designed to give all of the entities listed in 6 U.S.C. 321m(b)(1)(B) [3] (which we refer to as the ''listed entities''), as well as those who may seek to obtain voluntary certification, those who may seek to perform as certifying bodies, those who plan to develop private sector preparedness standards (including, for example, industry groups assembled for the purpose of developing such standards), and the public in general, additional opportunities to inform and consult with the designated officer on elements of PS-Prep. Anyone may submit comments on this guidance at any time, and comments will be considered as they are received. We would, however, appreciate any recommendations for adoption of currently-existing private sector preparedness standards within the next thirty (30) days, though we will accept submissions of private sector preparedness standards for adoption at any time.

III. DHS's Adoption of Voluntary Preparedness Standards

A. Call for Recommendations

In consultation with the listed entities, the designated officer is to ''adopt one or more appropriate voluntary preparedness standards that promote preparedness, which may be tailored to address the unique nature of various sectors within the private sector, as necessary and appropriate, that shall be used in the accreditation and certification program under this subsection.'' 6 U.S.C. 321m(b)(2)(B)(i). After initially adopting one or more standards, the designated officer may adopt additional standards or modify or discontinue the use of any adopted standard, as necessary and appropriate to promote preparedness. 6 U.S.C. 321m(b)(2)(B)(ii).

One of the main functions of this notice is to seek recommendations from the listed entities and the public at large regarding the private sector preparedness standards that DHS should adopt, both initially and over time. In order to facilitate those recommendations, we will discuss in the next sections the principles we plan to use in selection, and—in a question and answer format—the meaning of ''private sector preparedness standard'' and the elements that DHS will seek in such a standard.

We would appreciate any recommendations for adoption of currently-existing private sector preparedness standards within the next thirty (30) days, though we will accept submissions of private sector preparedness standards for adoption at any time. We note that the designated officer will consider adoption of the American National Standards Institute (ANSI) National Fire Protection Association (NFPA) 1600 Standard on Disaster/Emergency Management and Business Continuity Programs (ANSI/NFPA 1600)—the standard specifically mentioned in both the statute and the 9/11 Commission's recommendation—as well as any other private sector preparedness standards submitted for adoption.

B. Principles for Standards Adoption

The main principle informing DHS's adoption of standards is the main goal of the program: to widely encourage private sector preparedness through creation and use of voluntary standards. For this reason, PS-Prep is designed to maximize the number and type of private sector preparedness standards that DHS will consider adopting. While PS-Prep would consider adoption of—and strongly encourages the development and submission of—standards that contain all of the statutory elements of a private sector preparedness standard, and that could be applied generally to all entities in the private sector, PS-Prep will also consider more limited standards, such as those that apply to a particular industry or a subset of an industry, or those that cover a more circumscribed aspect of preparedness, such as business continuity planning.

A second principle is that the program is to be almost entirely driven by the private sector. While the designated officer, through the PSPCC, will adopt appropriate private sector standards, and manage the accreditation process through a non-governmental third party, the standards that are adopted are largely the product of private sector work—whether through voluntary consensus standards organizations, CIKR Sector Coordinating Councils, or other private sector entities. Private sector ingenuity is the lifeblood of the program. Understood this way, PS-Prep is a tool for both DHS and the private sector to give greater visibility—through a certification—to a private sector entity's conformity with a standard, and to more widely proliferate the use of standards in the private sector. It is emphatically not PS-Prep's purpose to impose a single federal preparedness standard on the private sector.

That said, the designated officer may modify or discontinue the use of any adopted standard, as necessary and appropriate to promote preparedness. Generally, the designated officer's review of adopted standards will be part of the annual programmatic review, discussed below.

A third principle—based upon both the scarcity of government resources and the need and wisdom of DHS using a risk-based approach in allocating those resources—is that the designated officer will have discretion to direct the PSPCC's adoption efforts at those private sector standards that meet needs identified by DHS. In other words, not all recommended private sector standards—and perhaps even not all appropriate recommended private sector standards—are guaranteed to be adopted by DHS.

[3] Those are ''representatives of appropriate organizations that coordinate or facilitate the development and use of voluntary consensus standards, appropriate voluntary consensus standards development organizations, each private sector advisory council created under section 102(f)(4), appropriate representatives of State and local governments, including emergency management officials, and appropriate private sector advisory groups, such as sector coordinating councils and information sharing and analysis centers.''

C. Elements to be Considered for DHS Adoption of a Standard

Given these principles, below is more specific guidance on standards that may be recommended to DHS for adoption.

What is a voluntary preparedness standard?

The Homeland Security Act defines a voluntary preparedness standard as ''a common set of criteria for preparedness, disaster management, emergency management, and business continuity programs, such as * * * ANSI/NFPA 1600.'' (6 U.S.C. 101(18)). We discuss our understanding of this definition below.

Will there be only one standard?

While we cannot predict how many standards DHS will ultimately adopt, the program is designed to consider and adopt multiple private sector preparedness standards, and encourage the development of additional standards, as well as the expansion and evolution of existing standards. In deciding which standards to adopt, the designated officer is required to consider standards that have already been created within the private sector, and to take into account the unique nature of various sectors within the private sector.

To use an example: if DHS were to adopt a general preparedness standard like ANSI/NFPA 1600, a facility such as a large shopping mall could seek certification of its preparedness plans and practices against that standard under PS-Prep. DHS might also adopt a more specific private sector preparedness standard covering that sector (commercial facilities) or subsector (shopping malls), if such a standard were created and if DHS determined it to be appropriate. In that case, the facility could seek certification under either standard, or under both.

PS-Prep will consider several types of voluntary private sector preparedness standards, and-though describing them before the private sector creates and proposes such standards would be unduly limiting-they can be broken down into two major divisions. First, DHS will consider adoption of standards that contain all of the statutory elements of a private sector preparedness standard, and that could be applied generally to all entities in the private sector. DHS will likely adopt such standards first, to provide the greatest chance for widespread adoption quickly. Such standards may contain modifications to take into account particular unique aspects of various industries and sectors, as well as currently-existing regulatory regimes that apply to those standards. Second, and importantly, PS-Prep will also consider more limited standards, such as those that apply to a particular industry or a subset of an industry, or those that cover a more circumscribed aspect of preparedness (i.e., an emergency preparedness standard for hospitals over a certain number of beds).

Will DHS only adopt ''consensus standards''*?*

Consensus standards, described in the Office of Management and Budget's Circular A–119, are so named because of the characteristics of their development process: openness, balance of interest, due process, an appeals process, and consensus.[4] We believe that consensus standards- and the consensus standards process-may yield some of the most valuable private sector standards for DHS to consider for adoption. But while the statute requires the designated officer to consult with ''voluntary consensus standards development organizations'' in managing the program, DHS is not limited in its adoption of standards to those developed in this fashion. In order to promote PS-Prep's goal of maximizing creation and adoption of private sector preparedness standards, standards developed by industry groups, non-profit organizations, and others—in addition to those developed by consensus standards development organizations—will be considered for adoption.

What is the difference between a ''standard'' and a ''plan''*?*

In discussing PS-Prep, there is sometimes confusion between ''plans'', which describe the preparedness practices and procedures that a private sector entity has in place, and ''standards'', which will be considered for adoption under the program. To clarify, practices and procedures are the things a private sector entity actually does to further its preparedness, and plans are an entity's description of what it does generally or what it will do in a particular situation. A certifiable private sector preparedness standard, on the other hand, is the yardstick against which a particular entity's practices, procedures and plans are measured.

Certainly, the boundary between standards and plans is not always well defined, and the PSPCC will review materials submitted for adoption to determine that they are, in fact, standards. Generally, however, PS-Prep will not consider for adoption a private sector entity's plan for preparedness, business continuity, emergency management, etc.—only the standards against which such plans and procedures are measured.

Must there be ''common elements'' in the standards adopted*?*

Private sector preparedness standards, according to the statutory definition, contain ''a common set of criteria'' for preparedness, disaster management, emergency management, and business continuity programs. We understand this to mean that the standard itself should have a common set of criteria for the private sector entities certified under it—not that all private sector standards in the program have the same criteria. Therefore, the designated officer will entertain adoption of private sector preparedness standards that cover one or more of the categories in the definition (i.e., preparedness, disaster management, emergency management, and business continuity programs), while also encouraging the development of standards that comprehensively incorporate disaster management, business management, and business continuity in a single framework.

Will certification be ''all or nothing''*?*

Some comments received to date have indicated that there is a desire for certifications on certain standards to be incremental (grading on a scale of conformance, for example) rather than absolute—sometimes called a ''maturity model process improvement approach.'' While certifications will, at least in the initial stages of the program, determine conformity or non-conformity with a particular standard, we welcome comments on this approach.

What is an ''appropriate'' standard*?*

The designated officer must determine that a preparedness standard is ''appropriate'' prior to adoption. 6 U.S.C. 324m(b)(2)(B)(i). For these purposes, an ''appropriate'' standard is one that the designated officer determines promotes private sector preparedness.

Included in this notice is a draft list of possible elements that can be included in private sector preparedness standards. It is, of course, not possible to devise uniform criteria that every standard submitted for adoption should meet—because, among other reasons,

[4] According to the circular, consensus is defined as general agreement, but not necessarily unanimity, and includes a process for attempting to resolve objections by interested parties, as long as all comments have been fairly considered, each objector is advised of the disposition of his or her objection(s) and the reasons why, and the consensus body members are given an opportunity to change their votes after reviewing the comments.

there may be industry-specific standards proposed, and standards may seek to address something less than the full range of matters that may be included in a preparedness standard. Even so, the list of possible elements included as Section XII below is a good starting point for parties developing private sector preparedness standards for adoption. A standard need not contain all of these elements to be appropriate and therefore be considered for adoption by DHS. Nonetheless, the list is provided to guide the private sector in developing appropriate standards, and will be modified as necessary.

IV. Accreditation

A. The Selected Entity

The designated officer is to:

> enter into one or more agreements with a highly qualified nongovernmental entity with experience or expertise in coordinating and facilitating the development and use of voluntary consensus standards and in managing or implementing accreditation and certification programs for voluntary consensus standards, or a similarly qualified private sector entity, to carry out accreditations and oversee the certification process under this subsection.

6 U.S.C. 321m(b)(3)(A)(i). On June 12, 2008, the designated officer entered into a contract with the ANSI-ASQ National Accreditation Board, or ANAB, to be the ''selected entity'' under the statute. As the selected entity, ANAB will develop and oversee the certification process, manage accreditation, and accredit qualified third parties to carry out certifications in accordance with the accepted procedures of the program. ANAB is an internationally recognized national accreditation organization, is an International Accreditation Forum (IAF) charter member, and currently is the only IAF-member accreditation organization for process/management system certifiers based in the United States.

B. Procedures and Requirements for the Accreditation Process

The designated officer is to develop guidelines for accreditation and certification processes (6 U.S.C. 321m(b)(2)(A)(ii)), and ANAB is to manage the accreditation process and oversee the certification in accordance with those procedures (6 U.S.C. 321m(b)(3)(A)(ii)).

Initially, ANAB will offer accreditation in accordance with an existing standard: International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC) Standard 17011, ''Conformity assessment—General requirements for accreditation bodies accrediting conformity assessment bodies.'' This standard establishes the general requirements for bodies accrediting entities that certify conformity with private sector standards. They are available at *http://www.ansi.org.* The designated officer will determine during the course of the PS-Prep program whether additional guidelines for accreditation beyond ISO/IEC 17011 are necessary, and DHS welcomes comment on this issue.

Application to become a certifying entity—known as a ''certifier''—will be voluntary and open to all entities that meet the qualifications of the PS-Prep program. To determine whether an entity is qualified to provide certifications, ANAB will consider whether the entity meets the criteria and agrees to the conditions—listed in 6 U.S.C.321m(b)(3)(F). These include important agreements about conflicts of interest.

C. Review of Certifiers

The designated officer and the selected entity shall regularly review certifiers to determine if they continue to comply with the program's procedures and requirements. 6 U.S.C. 321m(b)(3)(G). DHS will require the selected entity to review certifiers on at least an annual basis. A finding that a certifier is not complying with PS-Prep may result in the revocation of its accreditation. The designated officer will, when necessary and appropriate, review the certifications issued by any entity whose accreditation is revoked.

V. Certification of Qualified Private Sector Entities

Once ANAB accredits entities to provide certifications under the program, those certifiers will determine whether a private sector entity is, in fact, in conformity with one of the private sector preparedness standards adopted by DHS. The designated officer is to develop guidelines for certification (6 U.S.C. 321m(b)(2)(A)(ii)), and ANAB is to oversee the certification process in accordance with those procedures (6 U.S.C. 321m(b)(3)(A)(ii)).

Entities will certify based upon an existing standard: ISO/IEC Standard 17021, ''Conformity Assessment-Requirements for bodies providing audit and certification of management systems,'' available at *http://www.ansi.org.* After adoption of one or more standards, the designated officer and ANAB will work together to determine if there are any additional procedures that a certifier should use.

One important element of certification under any adopted standard is the following: As provided at 6 U.S.C. 321m(b)(3)(E), PS-Prep certifiers will, at the request of an entity seeking certification, consider non-PS Prep certifications. That is, the certifier may consider whether an already-acquired certification satisfies all or part of the PS-Prep certification requirement, and, if it does, the certifier may ''give credit'' for that pre-existing certification. This will avoid unnecessarily duplicative certification requirements.

VI. Small Business Concerns

Because the certification process may involve expense, and that expense may cause small businesses to avoid seeking certification, the statute calls upon the designated officer and the selected entity to ''establish separate classifications and methods of certification for small business concerns * * *.'' 6 U.S.C. 321m(b)(2)(D). DHS is considering several lower-cost options aside from third-party certification for small businesses. One such option is a self-declaration of conformity: an attestation by the small business that it has complied with one or more DHS-adopted standards. Another option is a second-party attestation, which would involve another entity—perhaps one that uses the small business in its supply chain—attesting that the small business is in conformity with one or more DHS-adopted standards. The DHS Ready-Business Program might be the appropriate portal for these self- and second-party attestations. DHS seeks comment on self-attestations of conformity, second-party attestations, and the employment of Ready-Business in this program, as well as any other proposal for alternatives allowing small business participation in PS-Prep.

Of course, only entities categorized as ''small business'' would be eligible to self-declare conformity, or for the other options described above. To determine which private sector entities are small businesses, the designated official will use the North American Industrial Classification System, or NAICS, which establishes a size standard for various industrial classifications. Additional information about NAICS is available at the Small Business Administration's Web site, *http://www.sba.gov/services/contractingopportunities/sizestandardstopics/index.html.*

VII. Other Relevant Issues

A. SAFETY Act

As mentioned above, DHS manages the Supporting Anti-terrorism by Fostering Effective Technologies Act of 2002 (SAFETY Act) Program. 6 U.S.C. 441–444; 6 CFR Part 25. The SAFETY Act Program is a liability mitigation

program intended to foster the development and the deployment of anti-terrorism technologies by providing certain liability protections to sellers and downstream purchasers of qualified anti-terrorism technologies, (QATTs).

While the determination of whether a technology should receive SAFETY Act protection is fact-specific, it is the case that private-sector preparedness standards submitted to DHS for adoption into PS-Prep may be determined to be QATTs. Similarly, the services provided by certifying entities may be determined to be QATTs as well. In considering the suitability of a preparedness standard for adoption under the PS-Prep process, DHS may ask questions similar to those asked in submission of a SAFETY Act application. Therefore, PS-Prep will seek to streamline the process for applying for SAFETY Act protection and PS-Prep's adoption of a private-sector preparedness standard, or accreditation as a certifying entity.

B. Access to Sensitive Information

Under PS-Prep, certifiers will be subject to confidentiality restrictions and will agree to use any information made available to them only for purposes of the certification process. 6 U.S.C. 321m(b)(3)(F)(vi). As mentioned above, DHS has a tool—the PCII Program—that may be useful in maintaining the confidentiality of sensitive information in the PS-Prep certification process. If any information that would be helpful to certifiers is Protected Critical Infrastructure Information as defined in 6 CFR Part 29—and if the private-sector entity seeking certification so requests—such information may be shared with the certifier while maintaining the protections of the PCII program. DHS will determine whether additional procedures are necessary for the use of PCII in the PS-Prep program.

C. Availability of Standards

We believe that the goal of encouraging creation and use of voluntary standards is best promoted if-once a standard is adopted into PS-Prep-it is made public, including through posting on the PS-Prep Web site. DHS welcomes comment on the proposed public availability of PS-Prep standards.

VIII. Public Listing of Certified Private Sector Entities

PS-Prep will maintain a publicly available list of private sector entities that have been certified as complying with one or more PS-Prep standards, and all certified entities that consent will be listed. This list will be posted on the PS-Prep Web site. This public listing will be of assistance to third parties-such as a business that has (or is planning to have) the certified entity in its supply chain-that need to know whether the entity has certain preparedness plans and procedures in place. Businesses that today must audit such entities- and in doing so incur the cost in time and labor of site visits, document review, and the like-may choose to rely on the public listing of PS-Prep certifications. Using PS-Prep in that fashion may reduce the costs associated with determining whether an entity has complied with a standard.

IX. Ongoing and Regular Activities of the PS-Prep Coordinating Council

The PSPCC is PS-Prep's decision-making body. It will, on an ongoing basis, determine DHS's priorities for adoption of private sector standards, recommend which standards should be adopted into the program based upon those priorities and the principles outlined in Section III, above, determine if additional guidelines for accreditation or certification are necessary, and interact with listed entities as required by the statute.

The PSPCC will also assist the designated officer in complying with the statutory requirement of an annual review. The statute requires the designated officer, in consultation with the listed entities, to annually review PS-Prep ''to ensure [its] effectiveness * * * and make improvements and adjustments to the program as necessary and appropriate.'' 6 U.S.C. 321m(b)(4)(A). The annual review is to include ''an assessment of the voluntary preparedness standard or standards used in the program under this subsection.'' 6 U.S.C. 321m(b)(4)(B).

While the annual review will serve as a time to determine whether additional private sector preparedness standards will be adopted into the program, we envision that the PSPCC will make determinations throughout the year as appropriate standards are submitted for consideration.

During the annual review, the PSPCC will also review the performance of the selected entity, and determine whether additional entities should be considered for that role.

XI. Next Steps

This notice is part of the consultation process with the listed entities, potential certifiers, entities that may seek certification, and the public at large. DHS has engaged in consultation prior to the issuance of this notice-including through speaking engagements, discussions in the normal course of business, meetings of the CIKR Sector Coordinating Councils, and the like- and will continue engaging with the public after the program is established.

DHS intends to hold two public meetings in Washington, DC to provide a forum for public comment, one in January and another in February, 2009. Meeting details and registration information will be published in the **Federal Register** and posted at *http://www.fema.gov/privatesectorpreparedness.*

While there may be additional notices related to PS-Prep, either in the **Federal Register** or on the PS-Prep Web site (including notices about the adoption of standards, the accreditation of certain entities, adoption or modification of accreditation or certification procedures, and the like), we do not plan to issue another notice before initial standards are adopted. Instead, we will-after careful review of the comments and recommendations for the adoption of one or more voluntary private sector preparedness standards-announce adopted standard or standards, as well as the logistics (such as whom to contact at DHS or the selected entity) of accreditation and certification. Comments on this guidance as well as recommendations of standards for DHS to adopt into the program may be submitted at any time.

XI. Draft List of Possible Elements To Consider in Standards Development

In order for DHS to adopt a standard to be part of PS-Prep, the designated officer must determine that it is ''appropriate.'' An appropriate standard is one that is determined by the designated officer to promote private sector preparedness.

Below is a draft list of possible elements that can be included in private sector preparedness standards and which may be used by the designated officer in evaluating standards for adoption in the program. The set of elements listed below can define the attributes of a comprehensive preparedness program. It is, of course, not possible to devise uniform criteria that every standard submitted for adoption should meet-because, among other reasons, there may be industry-specific standards proposed, and standards may seek to address something less than the full range of matters that may be included in a preparedness standard.

This list is a good starting point for parties developing private sector preparedness standards for adoption. A standard need not contain all of these elements to be appropriate and therefore

be considered for adoption by DHS, but the list is provided to guide the private sector in developing appropriate standards, and will be modified as necessary.

Possible Elements to Consider		Examples of how to satisfy element
Subject area	Elements and content	
1. Scope and Policy	A scope and/or policy statement that addresses preparedness, disaster management, emergency management, or business continuity. The standard may contain the following: 1. Scope. 1. Policy. 2. Principles. 3. Purpose.	1. Establish preparedness management program, including identification of appropriate resources and authorities. 2. Define scope and boundaries for development and implementation of the program. 3. Establish a framework for setting objectives, direction, and principles for action. 4. Demonstrate top management and the organization's commitment to preparedness management.
2. Requirements	A statement that the organization identifies and conforms to applicable legal, statutory, regulatory and other requirements (e.g., codes of practice and standards of care). The standard may contain the following, as well as a process for identifying and addressing them: 1. Legal. 2. Statutory. 3. Regulatory. 4. Other.	1. Identify, register and evaluate internal and external requirements pertinent to the organization's functions, activities and operations. 2. Understand potential impact of laws, regulations, codes, zoning, standards or practices concerning emergency procedures specific to the location and industry.
3. Objectives and Strategies.	The standard may contain requirements for strategies and/or strategic plans designed to accomplish the organization's objectives in: 1. Risk Management. 2. Incident Prevention. 3. Incident Preparedness. 4. Incident Mitigation. 5. Incident Response. 6. Business Continuity. 7. Incident Recovery. 8. Corrective and Preventive Actions.	1. Develop strategic plans for incident prevention, preparedness, mitigation, response, business continuity, system resiliency, and recovery for short term (less than a month) and long term (up to one year). 2. Identify type and availability of human, infrastructure, processing, and financial resources needed to achieve the organization's objectives. 3. Identify roles, responsibilities, authorities and their interrelationships within the organization required to ensure effective and efficient operations. 4. Plan the operational processes for actions required to achieve the organization's objectives. 5. Consider cyber and human security elements in control strategies and plans. 6. Make arrangements and contingency preparedness plans that should be in place to manage foreseeable emergencies. 7. Develop crisis communication plans with internal personnel (management, staff, response teams, etc.). 8. Ensure the company's Communications Department has identified key resources designated to initiate crisis communications with employees, business partners, vendors, government and external media. 9. Involve appropriate external parties during exercise events.
4. Risk Management	The standard may contain consideration of risk management, including hazard and threat identification, risk assessment, vulnerability analysis, and consequence/business impact analysis. The standard may provide for the conduct of: 1. Hazards and Threats Identification. 2. Risk Assessment. 3. Impact Analysis. 4. Vulnerability Assessment. 5. Consequence/Business Impact Analysis.	1. Establish a process for risk identification, analysis, and evaluation. 2. Identify assets, needs, requirements, and analysis of critical issues related to business disruption risks that are relevant to the organization and stakeholders. 3. Identify hazards and threats, to include cyber and human security elements. These should include loss of IT; telecommunications; key skills; negative publicity; employee or customer health or safety; damage to organization's reputation; loss of access to organization's assets; utility systems; supply chain outage/disruption, and insider threats. 4. Evaluate the probability of a disruptive event, dependencies and interdependencies with other assets and sectors, and consequences on business operations; Prioritize the issues identified as a result of the risk assessment and impact analysis. 5. Set objectives and targets (including time frames) based on the prioritization of issues within the context of an organization's policy and mission. 6. Evaluate and establish recovery time objectives. 7. Assess vulnerability of organization, systems, and processes. 8. Define risk treatment strategy and resources needed to address the organization's risks to business disruption.

Possible Elements to Consider		Examples of how to satisfy element
Subject area	Elements and content	
5. Operations, Control, and Risk Mitigation.	The standard may call for incident management / business continuity strategy, tactics, operational plans and procedures, and/or contingency plans that will be used during emergencies, crises and other events threatening its operation; and the documentation thereof. The standard may contain provisions for the following: 1. Operational Continuity. 2. Incident Management. 3. Coordination with Public Authorities.	1. Establish operational control measures needed to implement the strategic plan(s) and maintain control of activities and functions against defined targets. 2. Develop procedures for controlling key activities, functions, and operations associated with the organization, including possible large extended workforce absences; and alternative work sites or remote working procedures. 3. Establish processes and procedures for operational management and maintenance of infrastructure, plant, facilities, finance, etc. which have an impact on the organization's performance and its stakeholders. 4. Establish processes and procedures for management of documents which are essential to the successful implementation and operation of the preparedness management program or system. 5. Establish operational control measures needed to implement the strategic plan(s) and maintain control of activities and functions. 6. Develop insider threat mitigation measures. 7. Develop action plans for increased threat levels and tools to enhance situational awareness. 8. Formalize arrangements for those who supply and contract their services to the organization which have an impact on the organization's performance, including mutual aid agreements. 9. Determine the local and regional public authorities and their potential impact on your organization's plans including, but not limited to, the U.S. Department of Homeland Security, emergency management, fire, police, public utilities, and local & nationally elected public officials. 10. Work with local Public Information Officers to understand and follow protocol. 11. Document the forms and processes to be used before or during an event or exercise to ensure activities and participants, etc., are captured for review and Plan response and recovery improvements. 12. Collaborate with other organizations on preparedness issues of mutual concern.
6. Communications	The standard may call for plans for communication and warning as they apply to disaster/emergency management and business continuity. The standard may contain provisions for the following: • Warning and Notification. • Event Communication. • Crisis Management Communications. • Information Sharing. • Public Relations.	1. Develop and maintain a system required for communications and warning capability in the event of an incident/disruption. 2. Identify requirements, messages, and content required for communication within the organization. 3. Identify requirements, messages, and content required for external communication. 4. Develop, coordinate, evaluate and exercise plans to communicate information and warnings with internal stakeholders and external stakeholders (including the media) for normal and abnormal conditions. 5. Make arrangements for communications both within the organization and to/from external sources, including local, state and federal law enforcement and first responder organizations. 6. Document procedures and identify tools to manage relationships and communications processes with external partners: business partners, governmental agencies, vendors, etc.
7. Competence and Training.	The standard may call for review of the competence / qualifications and training of organization's personnel, contractors, and other relevant stakeholders involved in emergency management and business continuity management. The standard may contain provisions for the following: 1. Competence. 2. Training.	1. Assess, develop and implement training/education program(s) for the organization's personnel, contractors, and other relevant stakeholders. 2. Identify and establish skills, competency requirements, and qualifications needed by the organization to maintain operations. 3. Develop organizational awareness and establish a culture to support emergency / disaster preparedness and business continuity management. 4. Determine organizational interface protocol, identification and training requirements and assign appropriate internal staff or support representative(s).
8. Resource Management.	The standard may call for management and/or logistics plans, including allocation of human, physical, and financial resources in the event of incidents/emergencies that threaten operations. The standard may contain provisions for the following: 1. Resource Management. 2. Logistics and Business Processes.	1. Identify and assure availability of human, infrastructure, and financial resources in the event of a disruption. 2. Establish and document provisions for adequate finance and administrative resources and procedures to support the management program or system under normal and abnormal conditions. 3. Make arrangements for mutual aid and community assistance.

Possible Elements to Consider		Examples of how to satisfy element
Subject area	Elements and content	
9. Assessment and Evaluation.	The standard may call for assessments, audits and/or evaluation of disaster/emergency management and business continuity programs. The standard may contain provisions for Periodic Assessment and Performance Evaluation.	1. Establish metrics and mechanisms by which the organization assesses its ability to achieve the program's goals and objectives on an ongoing basis. 2. Determine nonconformities and the manner in which these are dealt with. 3. Conduct internal audits of system or programs. 4. Plan, coordinate, and conduct tests or exercises. 5. Evaluate and document exercise results. 6. Review exercise results with management to ensure corrective action is taken. 7. Report audits and verification results to chief executive officer.
10. Continuing Review (ongoing management and maintenance).	The standard may call for a plan for program revision and process improvement, including corrective actions. The standard may contain provisions for the following: 1. Review. 2. Maintenance. 3. Process improvement.	1. Conduct management review of programs and/or system to determine its current performance, to ensure its continuing suitability, adequacy and effectiveness, and to instruct improvements and new directions when found necessary. 2. Make provisions for improvement of programs, systems, and/or operational processes.

Dated: December 18, 2008.

R. David Paulison,

Administrator, Federal Emergency Management Agency.

[FR Doc. E8–30685 Filed 12–23–08; 8:45 am]

BILLING CODE 9110–14–P

DEPARTMENT OF HOMELAND SECURITY

Transportation Security Administration

Intent To Request Renewal From OMB of One Current Public Collection of Information: Department of Homeland Security—Vulnerability Identification Self-Assessment Tool—Transportation (DHS–VISAT–T)

AGENCY: Transportation Security Administration, DHS.

ACTION: 60-day notice.

SUMMARY: The Transportation Security Administration (TSA) invites public comment on one currently approved Information Collection Request (ICR), OMB control number 1652–0037, abstracted below. TSA plans to submit the renewal request to the Office of Management and Budget (OMB) in compliance with the Paperwork Reduction Act. The ICR describes the nature of the information collection and its expected burden. The collection involves the voluntary submission of information regarding currently deployed security measures, through a self-assessment tool, from transportation sectors so that TSA can prioritize resources.

DATES: Send your comments by February 23, 2009.

ADDRESSES: Comments may be mailed or delivered to Ginger LeMay, Office of Information Technology, TSA–11, Transportation Security Administration, 601 South 12th Street, Arlington, VA 20598–6011.

FOR FURTHER INFORMATION CONTACT: Giner LeMay at the above address, or by telephone (571) 227–3616 or e-mail *Ginger.LeMay@dhs.gov*.

SUPPLEMENTARY INFORMATION:

Comments Invited

In accordance with the Paperwork Reduction Act of 1995 (44 U.S.C. 3501 *et seq.*), an agency may not conduct or sponsor, and a person is not required to respond to, a collection of information unless it displays a valid OMB control number. The ICR documentation is available at *http://www.reginfo.gov*. Therefore, in preparation for OMB review and approval of the following information collection, TSA is soliciting comments to—

(1) Evaluate whether the proposed information requirement is necessary for the proper performance of the functions of the agency, including whether the information will have practical utility;

(2) Evaluate the accuracy of the agency's estimate of the burden;

(3) Enhance the quality, utility, and clarity of the information to be collected; and

(4) Minimize the burden of the collection of information on those who are to respond, including using appropriate automated, electronic, mechanical, or other technological collection techniques or other forms of information technology.

Information Collection Requirement

OMB Control No. 1652–0037; Department of Homeland Security—Vulnerability Identification Self-Assessment Tool—Transportation (DHS–VISAT–T). After its inception TSA faced the challenge of enhancing security in all modes within the transportation sector. A methodology was required to support inter- and intra-modal analysis and decision-making. Millions of assets exist within the transportation sector, ranging from over 500,000 highway-bridges and approximately 4,000 mass transit agencies, to over 19,000 general aviation airports. Given this population of assets, in order to prioritize resources, TSA needs to continue to collect data from the asset owners or operators on security measures deployed and their effectiveness.

In response to this need, TSA's Office of Intelligence/Risk Support Division developed the Department of Homeland Security—Vulnerability Identification Self-Assessment Tool—Transportation (DHS–VISAT–T), formerly called the TSA Self-Assessment Risk Module (TSARM), as a means to gather security-related data and provide a cost-free service to the transportation sector. TSA designed this tool to be flexible to support the unique characteristics of each transportation mode, while still providing a common framework from which analysis can be conducted and trends can be identified. Thus far, TSA has developed modules of the tool for maritime, mass transit, highway bridges, and rail passenger stations, with more in development.

DHS–VISAT–T represents the U.S. Government's first self-assessment tool that guides a user through a series of security-related questions to develop a comprehensive baseline evaluation of a transit agency's current level of security. The tool provides the following features: