

**Before the
FEDERAL EMERGENCY MANAGEMENT AGENCY
Washington, D.C. 20472**

In the Matter of)
)
Voluntary Private Sector Accreditation and) Docket ID FEMA-2008-0017
Certification Preparedness Program)

COMMENTS OF ASIS INTERNATIONAL

ASIS International (ASIS) submits these comments in response to the Federal Register Public Notice released October 16, 2009, in the above referenced docket. ASIS is the largest organization for security professionals, with more than 37,000 members worldwide and an American National Standards Institute (ANSI) Accredited Standards Development Organization (SDO).

These comments are in response to the notice published in the Federal Register Vol.74, no. 199/Friday, October 16, 2009/Notices Docket ID FEMA 2008-0017. We appreciate this opportunity to present comments and recommendations to DHS as it considers which standards to designate for the PS-Prep Program.

Question 1. Are there reasons that DHS should not adopt any one of the three standards listed above?

No. Perhaps an alternative question is: “why only these three standards?” The intent of the PS-Prep Program is to promote “preparedness” in the private sector. We fully concur with the recommendations of the Sloan Report prepared by ASIS International (ASIS), Disaster Recovery Institute International (DRII), National Fire Protection Association (NFPA), Risk and Insurance Management Society, Inc. (RIMS) that:

“It is important for the DHS to recognize that multiple approaches comply with the spirit of Title IX of PL 110-53. Therefore, greater resiliency success will be achieved if businesses are given the freedom and flexibility to determine how they will improve preparedness in a way that best fits their respective business models.” and

“For the private sector to adequately and voluntarily establish preparedness programs, it should be given the flexibility to choose from various standards, guidelines and best practices that best meet the respective organization’s needs for preparedness.”

In addition to the three designated standards, the private sector has been using other standards, guidelines and best practices for quite some time to improve their preparedness. ISO27001, ISO28000, RAMCAP, and enterprise risk management approaches have been successfully used by many private sector organizations to address preparedness and continuity management before the introduction of the ASIS and BSI standards. The PS-Prep program should incentivize organizations to use what works best for them to improve preparedness, not place a barrier of third-party certification to a choice only three standards.

The three standards chosen represent three distinct approaches to preparedness, any of which can improve preparedness. The ASIS standard takes a holistic management system approach that helps an

organization to cost-effectively manage risk by developing balanced strategies to adaptively, proactively and reactively address minimization of both the likelihood and consequences of disruptive events. The BSI and NFPA standards focus on consequences of disruptive events. The BSI standard is business continuity-centric and uses a management systems approach, while the NFPA standard is more emergency management-centric and takes a check-list approach without introducing a management system. The choice of which standard to use is a matter of taste and what fits a company's business and management style. They all help improve preparedness, so any of the three standards identified in the Federal Register should be adopted by the PS-Prep program. (However, the BSI standard should also be available for free download, as is currently the case for the ASIS and NFPA standards.)

Question 2. Are there any supporting guidance materials in addition to the three identified standards that are needed to help the private sector attain certification to one of the three standards?

Again, quoting the Sloan Report:

“What is lacking in preparedness management is the rich amount of training materials, case studies, tool sets, technical assistance and peer programs that have been developed over time to help small and medium companies meet these contractual requirements for environmental management.

The next effort should concentrate on creating tools to evaluate existing programs, and developing training materials, case studies, tool sets, technical assistance and peer programs to assist small and medium businesses develop and enhance their preparedness programs. The challenge is how to implement the above approaches in a cost-effective fashion. For the private sector to improve preparedness performance, it needs the tools and knowledge how to address the core elements in a business sensible fashion. Much can be learned from the decades of experience in quality and environmental management, particularly tailoring approaches that address the needs of small and medium businesses.”

The ANSI/ASIS ASIS SPC.1-2009 has a significant advantage in terms of supporting guidance materials, because of the three designated standards it is the one that is 100% compatible with existing ISO standards.

The ANSI/ASIS.SPC.1:2009 is business friendly by following exactly the ISO management systems approach. It is:

- Aligned with the globally accepted standards:
 - ISO 9001:2000 - Quality management
 - ISO 14001:2004 - Environmental management
 - OHSAS 18001:2007 - Occupational health and safety
 - ISO/IEC 27001:2005 - Information technology security
 - ISO 28000:2007 - Security management systems for the supply chain
 - ISO 31000:2009 – Risk Management
- Supports consistent and integrated implementation and operation with related management standards.
- One suitably designed management system can satisfy the requirements of all these standards.

- The auditing process for the ANSI/ASIS.SPC.1:2009 is 100% consistent with the decade's proven ISO management system standards auditing process. Therefore, Lead Auditor certification and competency can be based on existing ISO standards.
- Is aligned with the new ISO 31000:2009 – Risk Management which allows to the organization to better integrate preparedness into its overall risk management strategy.
- Enables the the private sector to tap the vast amount of of guidance information generated over the past two decades on implementation and operation of ISO management systems (much of which was paid for by the US government). Organizations can easily jumpstart their preparedness program building on lessons learned and using tools developed for the other ISO standards, much of which was developed specifically for small and medium sized enterprises.

By building on the existing ISO model, organizations can leverage their existing management systems. While organizations new to this arena can use the knowledge base, much of it free for download from the Internet, to phase in elements of the standard in a continual improvement cycle towards full conformance with the standard.

Question 3. What factors would a business consider in determining which DHS adopted standard(s) to pursue for certification under the PS-Prep Program?

Adoption of a standard should not be based on pursuing certification, it should be based on what best fits the organization's business mission, objectives and management style. The focus should be on which standard will help the organization improve its preparedness performance. Certification should only enter into consideration if there is a compelling business case to do so.

For most businesses, first or second party validation and certification would probably be sufficient without the expense of external third party certification. Indeed, second party certification that is contractually enforced has significant advantages over external third party certification for most organizations, particularly small and medium sized enterprises. DHS (or Congress) should consider modifying the program to encourage improvement of preparedness performance by recognizing first and second party certification. This program should be solely focused on better preparedness in the private sector and United States will benefit from the organizations becoming better prepared more so than generating revenue for consultants and certification bodies.

DHS should view the question of certification from the perspective of how can the PS-Prep program fit into the decades tested and proven certification scheme used with ISO standards. If third party certification is pursued, the approach should be identical to that used by the ISO 9001 and ISO 14001 to assure the transparency and integrity of the certification process. All the applicable ISO standards related to auditing and certification should be strictly adhered to, as well as the method used by reputable certification bodies that only work with RABQSA and IRCA certified Lead Auditors.

Question 4. What are the reasons for businesses to seek certification under these identified standards?

There is only one reason a business seeks certification under any standard, business advantage. Business advantage is a function of the organization's business mission and its internal and external operating environment. This is why the third party certification requirement of the PS-Prep program is misguided. As with other standards, more companies use standards to improve their performance,

with first or second party validation providing sufficient cost-benefit advantage to pursue implementation of the standard.

Companies doing business in the international arena have a clear business advantage of adopting an ISO, or ISO-like standard, or a standard shared as a national standard by various countries. Certification to a standard should also be done with international credibility and acceptance in mind. The ASIS standard has the distinct advantage of being an exact clone of an ISO standard. In fact, it can be used to satisfy all the requirements of the ISO28000, and the management system requirements for the ISO9001, ISO14001, OHSAS18001, and ISO27001. This not only lends credibility, but enables integrated application and joint auditing, a significant cost savings. Furthermore, the ASIS standard has already been adopted by countries as National Standards in Europe (ratified in Denmark and the Netherlands) and is in the process of adoption in National Technical Committees in other European countries, as well as in Africa and the Pacific Rim.

Question 5. How would the fact that an organization is certified under the PS-Prep Program affect or otherwise influence your decision to do business with them?

Standards are supposed to be market-driven by the private sector. If implementation, maintenance and validation of conformance of a standard are done in an honest, transparent and credible way, government involvement and recognition is immaterial. The world market recognizes the credibility of the ISO management system standards and the ISO conformance assurance system. This is the internationally recognized quality assurance system. Therefore, if DHS would like the PS-Prep program to have market credibility they only need to adopt the ISO system that has already proven its market power. Furthermore, if DHS encourages organizations to use RABQSA and IRCA certified Lead Auditors for internal audits and second party certification, first and second party approaches will also have sufficient credibility for market acceptance.

For larger organizations that have teams of internal RABQSA and IRCA certified Lead Auditors, there is no incentive to certify under the PS-Prep program. They have an internal mechanism for continual improvement of preparedness and will rarely be able to justify the cost of third party certification nor the risk introduced by sharing their risk assessment and impact analysis with an external body.

Question 6. In response to the December 2008 Federal Register notice, DHS received numerous comments promoting the use of a “maturity model process improvement approach” for business preparedness and continuity. The maturity model was described as an approach whereby certifications on certain standards could be incremental, i.e., grading on a scale of conformance, rather than a conformance/non-conformance basis. The notice noted that certifications will determine conformity or non-conformity with a particular standard. How could the use of a maturity model approach be applied to certification to any of these standards?

Maturity models or phased implementation models have been successfully used for many ISO standards, but this is for demonstrating continual improvement of performance, not used as a substitute for certification. A phased approach to implementing a management systems standard with a driver of continual improvement based on the Plan-Do-Check-Act model can be viewed as a maturity model. Since the ASIS and BSI standards are management systems based on a PDCA model, they have built into them a maturity model approach.

The problem is an over emphasis on external third-party certification. If DHS was to waive the external third-party certification and government recognition aspects of this program, businesses could focus on continual improvement of preparedness. Private sector organizations large and small could adopt maturity models or phased implementation models that fit the business realities in which they operate and fulfill the intent of the law, strengthening US private sector preparedness.

Question 7. What may be the potential impact (e.g., cost, return on investment, other considerations, etc.) on small businesses when attempting to implement any of the above identified standards?

Absent of the certification requirements, any of the identified standards can be used by small business to benchmark and continually improve their preparedness performance. Third party certification is a barrier to small and medium sized businesses and is counterproductive to encouraging private sector preparedness. Businesses should be given the freedom and flexibility to determine how they will improve preparedness in a way that best fits their respective business models without looming external third party certification provisions. Small businesses need to tailor their preparedness and resilience strategies to their financial realities.

In the programs current form, small businesses may fall prey to consultants, training organizations, and certification bodies willing to steer them on a path of least resistance to quick certification rather than continual improvement of their business and preparedness. Moreover, there are no documented benefits of external third party certification at this time, so there is no clear business case to justify the expense of certification, as well as the maintenance of certification (a significant on-going expense) for businesses of any size. Also, what happens to small businesses that implement and maintain the standards, but cannot justify the on-going expense of maintenance of external third-party certification? Will these businesses be stigmatized for switching to a first or second party demonstration of conformance to continually improve their preparedness?

The major barrier to preparedness and resilience management is a lack of knowledge and tools, particularly in case of small businesses. DHS would better serve small businesses and help link preparedness to return on investment by supporting development of tools, case studies, mentoring programs, and the knowledge base for implementing all or parts of the standards, similar to what the EPA did to promote improved environmental management. In fact, DHS could leverage the huge investment of taxpayers' dollars that EPA received to promote environmental management in the private sector by extracting relevant lessons learned and applicable materials, tool sets, and programs.

Thank you for the opportunity to comment on the standards DHS intends to adopt for the PS-Prep program.