



August 15, 2008

Dear Sir/Madam:

Re: Comments to ASIS ANSI PINS Standards Project - BSR ASIS BCM.01-200X

Thank you for your interest in the ASIS International (ASIS) Business Continuity Management Standards Project. ASIS International is the official name of the organization conducting this standards development project. The ASIS organization name was formally changed from the American Society for Industrial Security in 2002.

ASIS, an American National Standards Institute (ANSI) accredited Standards Developing Organization (SDO), has filed an ANSI Project Initiation Notification System (PINS) Form with the intention to develop a business continuity management system standard using the internationally recognized and proven method of a process approach with the Plan-Do-Check-Act (PDCA) model. As you may be aware, this is an approach used in all ISO management system standards to enable integrated application of standards and avoid siloing of risks. This is a well known globally recognized business approach. There is no American National Standard or ISO Standard in existence today for a management system standard addressing business continuity.

The ANSI PINS, per the ANSI Essential Requirements, is the means of notification of standards development and coordination. Per the ASIS Standards Developing Operating Procedures, ASIS complies with ANSI's PINS requirements and is in the early stages of developing the business continuity management system standard as a proposed American National Standard. There will be extensive reach out to materially and affected interested parties as is required in the standards development process. Contrary to the DRII release, (see Attachment I), ASIS has not created a standard on business continuity management and has not moved forward on any unapproved standard with ANSI. Any attempt of this nature is not feasible per the ANSI Essential Requirements, the ASIS Standards Operating Procedures or in the standards development process for that matter. To be exact, ASIS is following the appropriate processes for standards development in the United States, through the ANSI PINS to initiate the standards development process. The PINS serves as a public announcement in an attempt to notify potentially interested parties of the standards activity and allow for the recruitment of participation from interested parties who will use the proposed standard and will be affected by it. Interested parties should contact ASIS in this regard, copying ANSI at one's discretion. (It is noted here that the DRII release has the mistaken ANSI point of contact information.)

From the comments submitted, it is presumed you are interested in this standards development project and your participation is most welcome. The PINS announcement is a call to the business continuity community and other interested and affected parties to participate in the creation of the standard. A technical committee will be formed shortly and we welcome your participation.

As you may be aware, the US Department of Homeland Security (DHS) recently stated that no one standard (management system standard or otherwise) currently exists that addresses the program requirements of Title IX of H.R. 1 and Public Law 110-53 "Implementing recommendations of the 9/11 Commission Act of 2007". (DHS Private Sector Office and the Office of Infrastructure Protection tele-briefing on the voluntary preparedness standards and certification program, July 31, 2008). ASIS, as an ANSI accredited standards developer and SDO, recognized this issue prior to the DHS statement and as a result initiated the standards development process by issuing the ANSI PINS.

Please note that DRI International (DRII) is not an ANSI accredited SDO. Therefore, they cannot develop and/or publish American National Standards. The DRI International Professional Practices, which forms the basis for the DRII certifications, is not an American National Standard or an ISO Standard, nor have they met the specific criteria of either the ANSI or ISO standards development processes. As you may know, standards development is a well choreographed process under the directorship of organizations such as ANSI, ISO and CEN. ASIS International, an accredited SDO, participates in both national and international standards development activities according to the rigor of strictly defined protocols. Unfortunately, in the United States, and other countries, many organizations who are not SDO's refer to their

proprietary best practices as “standards”. This causes much confusion in an ever changing landscape. We anticipate that when the ISO standard for preparedness and continuity management is published it will level the playing field by making a single international standard that will facilitate trade and business.

ASIS International is an association of over 36,000 members with 205 Chapters in 46 countries. We have a membership presence in over 200 countries. We are well aware of the problem of conflicting national standards. This is exactly why ASIS International has adopted the ISO approach to standardization. It is our view that the time-proven model developed by ISO in other management system standards facilitates trade and minimizes the burden on individual countries and organizations.

We would like to point out that ASIS, as an organization, is not, and never has been, a member of the NFPA 1600 Technical Committee.

The NFPA 1600 provides a list of multiple plans one needs to create for emergency/disaster management, while the ASIS standards project described in the ANSI PINS incorporates a management process approach using the PDCA model giving a single management system that incorporates and connects policies, strategies, resources, and plans. The PDCA approach is the globally accepted approach compatible with management system standards for quality, environment, occupational health and safety, food safety, information security and supply chain security thus also making it consistent with a more general enterprise risk management approach. The NFPA 1600 being devoid of a management system is not directly compatible. It should be noted that the Canadians recently released the Canadian standard Z-1600 to replace the NFPA 1600 due to the NFPA 1600's lack of a PDCA approach. Compatibility with existing management system standards using the PDCA model is the global trend, which is being adopted in all ASIS standards activities.

The NFPA 1600 is written by the National Fire Protection Association from a first responder's perspective and mainly focuses on emergency/disaster response and planning rather than a business continuity management approach of protecting critical assets, functions, services and products. The NFPA 1600 appears to be an emergency/disaster response and planning standard with minimal reference to analyzing and understanding the business.

We would like to point out DRII's published position of January 18, 2008: *“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. Organizations that have implemented preparedness management controls, best practices or complementary systems which address the core elements should be recognized and “credited” as demonstrating preparedness. Regulated industries should be given credit for their compliance with relevant regulations without the need for duplicative systems.”* Source: Framework for Voluntary Preparedness - Briefing Regarding Private Sector Approaches to Title IX of H.R. 1 And Public Law 110-53 “Implementing Recommendations of the 9/11 Commission Act of 2007”. Prepared for the Alfred P. Sloan Foundation by ASIS International (ASIS), Disaster Recovery Institute International (DRII), National Fire Protection Association (NFPA), and Risk and Insurance Management Society, Inc. (RIMS).

Your participation is strongly encouraged in the development of the business continuity management standard as it is important to have as much as possible a breadth of subject matter professionals, the respective communities that they serve and other affected and interested parties. It is unfortunate that misinformation may have led to uncertainty. Please advise if you wish to serve on the technical committee that will be established after the public announcement stage of the PINS by way of contacting Susan Carioti ([scarioti@asisonline.org](mailto:scarioti@asisonline.org)).

Sincerely yours,

**[Original Signed by]**

F. Mark Geraci  
Chairman, Standards and Guidelines Commission  
ASIS International

Attachment

cc: Susan Melnicove, ASIS International Vice President, Education  
Susan Carioti, ASIS International Director, Standards and Guidelines  
Marc Siegel, ASIS International Security Management Systems Consultant  
Anne Caldas, ANSI Director of Procedures and Standards Administration

## DRI International

Urgent Action Required

### IMMEDIATE ACTION IS REQUIRED

**Your assistance is urgently needed to preserve the integrity of BCP standards.**

**Washington, DC - August 12, 2008** - Last October, Disaster Recovery Institute International (DRI) issued a position statement regarding the establishment of a standard for Business Continuity Planning. This was in response to the American Society for Industrial Security (ASIS) attempting push through an unproved and ill-considered standard with the American National Standards Institute (ANSI). We believed that our statement had settled the matter.

However, ASIS has filed two notices with the ANSI called "PINS Forms: Standards Action Public Review Requests." One of these is "BSR/ASIS BCM.01-200x, Business Continuity Management: Preparedness, Crisis Management, and Disaster Recovery". This proposed standard is being drafted "to include **auditable** criteria for preparedness, crisis management, business/operational continuity and disaster management using a process approach with the Plan-Do-Check-Act model, as required by Title IX of H.R. 1 and Public Law 110-53 'Implementing Recommendations of the 9/11 Commission Act of 2007'".

DRI International strongly opposes this filing. We are asking our colleagues and certified professionals in the field to oppose this effort to create a "Business Continuity Management" standard in an industry already beset with multiple and often confusing standards. The comment period for this "PINS" phase of "BSR/ASIS BCM.01-200x" closes on **August 30, 2008**.

Please send a clear message to ANSI through its designated point of contact, [Susan Carioti at scarioti@asisonline.org](mailto:SusanCarioti@asisonline.org). We are making every attempt to coordinate this effort and track the comments, which we believe will help in making presentations to ANSI and other appropriate agencies. When you send your e-mail to Ms. Carioti, please send a bcc to standards@drii.org. Your efforts are greatly appreciated.

### Suggested Comments for Response

#### **Doesn't a standard for Business Continuity practices already exist?**

Yes. NFPA 1600 - Standard on Disaster/Emergency Management and Business Continuity Programs has been the US and Canadian standard for Business Continuity since 1995. NFPA 1600, DRI International Professional Practices and BCI's Certification Standards for Professional Practitioners form the basis for the certifications held by the majority of the world's certified Business Continuity professionals.

#### **Is NFPA 1600 recognized outside the Business Continuity community?**

Yes. It is the standard endorsed by the U.S. Department of Homeland Security and the

Federal Emergency Management Agency and certified as an ANSI Standard.

**Was ASIS given an opportunity to have their opinion heard?**

Yes. But, ASIS had an opportunity to provide input to NFPA 1600, as a member of NFPA's Technical Committee, but ASIS declined.

**Were BC Professionals involved in creating this standard?**

No. ASIS created a "standard" that serves the needs of the security profession without the benefit of comment from DRI International, BCI, RIMS, NFPA and other recognized subject matter experts. ASIS has never approached the business continuity industry itself to participate in the creation of its draft standard.

**What's wrong with independent standards?**

Briefly, the continuing creation of independent standards in these areas does little more than generate confusion in fields that are already beset with multiple standards and definitions. Such efforts serve only to increase the "noise" in an industry that is already far too difficult for even experienced practitioners to explain to those who look to us to help them manage the complex array of risks that we all face in today's environment.

**If a standard needs to be created, how should it be done?**

True "standards" come about as the result of communication and collaboration involving experts in the subject matter area to which the particular standard is to apply. This is the only way to ensure that the standards that are created represent a consensus that will be of benefit to both the subject matter professionals and the respective communities that they serve.

[Forward email](#)

✉ [SafeUnsubscribe®](#) [rwooldridge@drii.org](mailto:rwooldridge@drii.org).