



January 14, 2010

Via E-Mail: [DHS-POLICY@dhs.gov](mailto:DHS-POLICY@dhs.gov)

Office of Chief Counsel  
Federal Emergency Management Agency  
500 C St., SW, Room 840  
Washington, DC 20472-3100

Re: Voluntary Private Sector Accreditation and Certification Preparedness Program (Docket ID DHS-2008-0017)

Dear Sir or Madam:

The Securities Industry and Financial Markets Association (“SIFMA”)<sup>1</sup> Business Continuity Committee (“Committee”) appreciates the opportunity to provide comments on the Voluntary Private Sector Accreditation and Certification Preparedness Program (“PS-Prep Program”). SIFMA applauds DHS’s efforts to create a voluntary certification program, and hopes any such program will take into account the substantial regulatory regime which already exists for SIFMA’s member firms and give such firms credit for their existing compliance programs. The Committee is providing below general comments, as well as responses to the specific questions for comment in the release.

## 1. General Comments

As financial institutions, SIFMA members are currently subject to many levels of regulation and examinations related to business continuity planning (“BCP”) programs, including the Securities and Exchange Commission (“SEC”), the Federal Reserve (“Fed”), Department of the Treasury (“Treasury”) and the Financial Regulatory Authority (“FINRA”). These regulatory regimes have strict standards which apply to all regulated entities which meet or exceed all of the primary

---

<sup>1</sup> The Securities Industry and Financial Markets Association (SIFMA) brings together the shared interests of hundreds of securities firms, banks and asset managers. SIFMA’s mission is to encourage strong financial markets, capital availability, job creation, and economic growth, while building trust and confidence in the financial industry. SIFMA, with offices in New York and Washington, D.C., is the U.S. regional member of the Global Financial Markets Association (GFMA). For more information, visit [www.sifma.org](http://www.sifma.org).

standards in the PS-Prep Program. In addition, many firms have adopted best practices which include extensive third-party audits of their BCP programs.

As a result, the Committee questions what value member firms would place on obtaining the PS-Prep Program certification because many firms are already required to comply with rigorous BCP regulations. So long as the program remains truly voluntary, this is a conclusion that many firms may reach particularly in light of the costs firms would undertake to obtain the certification. Such costs would be increased by the requirement to satisfy multiple standards. At a minimum, we believe our members should be given credit for compliance with existing applicable regulatory standards when applying for the certification.

In addition, the Committee believes that prior to implementing any PS-Prep Program, DHS should clarify the scope of the program by taking into account the relative diversity of size, resources, and criticality of private sector entities. DHS should also clarify how large multinational or multi-division companies would seek certification. For example, would each business unit need to be certified, or could the corporate parent be certified and such certification would apply to all of the subsidiary companies and divisions?

Finally, SIFMA believes the BCP-related regulations governing Critical Infrastructure and Key Resources (CIKR) sectors should be analyzed *prior* to the adoption of the initial PS-Prep Program standards and not after. The Committee would be happy to have a meeting with DHS to discuss these standards and the applicable regulations governing the financial services industry.

## **2. Responses to Requests for Comment**

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

SIFMA does not have a specific objection to any one of the standards listed in the PS-Prep Program proposal, but notes that they are not all the same. DHS should take note that the *NFPA 1600 – Standard on Disaster / Emergency Management and Business Continuity Programs* (“NFPA 1600”) does not include a self-assessment and does not have the “plan-do-check-act” methodology that the others have.

DHS should also consider how new versions of the standards will be treated. For example, we understand the NFPA is expected to release a new version of NFPA 1600 shortly. Those seeking certification would need to know whether to follow the 2007 standard or the 2010 standard.

*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?*

SIFMA notes that the *BS25999 – Business Continuity Management* standard has a methodology book that needs to be studied prior to implementing the standard. NFPA has also issued a Handbook relating NFPA 1600. Firms would have to pay to get these materials and those costs should be considered. Also, review courses are available for training individuals to keep standards effective within their companies.

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

The Committee believes that firms would consider a variety of factors in determining which standard to follow, particularly the costs involved, the ability to maintain the certification, competitive advantage (if any), regulatory direction, ease of adoption in light of existing programs, ease of compliance with the standard, and the credibility of the program domestically and internationally.

*4) What are the reasons for businesses to seek certification under these identified standards?*

The Committee believes that firms would perform a careful cost/benefit analysis using many factors prior to embarking on the PS-Prep Program certification process. SIFMA believes there will be substantial time and costs involved with such analysis, but the benefits are not yet clear. Firms may seek the certification for the following reasons: improved disaster preparedness, endorsement by financial regulators, competitive advantage, and reputational gain.

*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?*

The Committee believes that certification of a vendor under the PS-PREP program could have some effect on selection of a vendor, but it would not be an overriding factor in selecting or rejecting a vendor. Under current regulations, securities firms must assess the recovery capabilities of their critical vendors and firms also have assessment methodologies in place. In many cases, this analysis is more rigid than the PS-PREP standards and would be given greater emphasis. Where a firm relies on a less rigid standard, a vendor's compliance with PS-PREP could be helpful.

SIFMA would welcome DHS guidelines relating to tangible, measurable metrics for inclusion in contracts and service-level objectives with our essential external third-party vendors and service providers. These metrics should apply to all aspects of the business continuity management life-cycle.

*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?*

SIFMA does not believe the use of a maturity model against one of the standards would be helpful. The standards selected are designed to be binary in nature (Pass/Fail), so there is no "partial compliance" rating for any of the three selected. Most of the maturity models would use a standard as part of a rating against the model itself. Adoption of a standard using a maturity model does not provide compliance against a standard and does not fulfill the spirit of this program.

*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?*

The Committee believes the PS-Prep certification could have varied effects on small businesses. We note that the proposal does not seem to include a definition of a small business which makes this question somewhat difficult to properly answer.

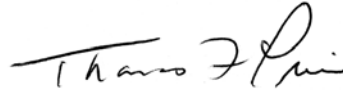
The most detrimental effect this could have on small business is the potential cost incurred to receive the certification. Many small securities firms may have only one BCP professional on staff and this person most likely performs other functions within their firm or is a part-time consultant. It may also be cost-prohibitive to maintain the infrastructure required to maintain the certification.

As noted above, however, there may be some benefit for small businesses when analyzing whether vendors or other business partners have adequate BCP programs in place. Ultimately, whether to voluntarily pursue the certification would likely be based upon each individual firm's cost/benefit analysis.

\* \* \*

Thank you for the opportunity to respond to these questions. If you have any questions or require additional information, please contact Howard H. Sprow, Vice President Technology & BCP at 212-313-1248.

Regards,

A handwritten signature in black ink that reads "Thomas Price". The signature is written in a cursive style with a long horizontal stroke at the beginning.

Thomas Price  
Managing Director  
Operations, Technology & BCP