



# The Business Reporting Working Group

## On the Voluntary Business Preparedness Accreditation and Certification Program

Hosted by:  
International Center for Enterprise Preparedness (InterCEP)  
New York University

Initial Meeting  
March 28, 2008

### DRAFT SUMMARY PROCEEDINGS

(6/12/08 Version)

#### Table of Contents

	<i>Section</i>	<i>Page #</i>
Executive Summary		2
About InterCEP		3
Meeting Agenda		3
Ground Rules		3
Overview of New Law		3
U.S. Department of Homeland Security's Responsibilities		4
Current Status		4
The Working Group Initiative		4
The Business Reporting Perspective		5
Discussion Points		5
InterCEP's Activities		7
Setting the Working Group Agenda Moving Forward		8

## EXECUTIVE SUMMARY

On March 28, 2008 a diverse group of private sector representatives and other stakeholders convened in an initial online forum of the Business Reporting Working Group to discuss rating agency issues pertaining to the voluntary business preparedness accreditation and certification program currently under development pursuant to US federal legislation.

The discussion focused on the following key issues:

- **Participants acknowledged the importance of making sure that the voluntary certification program incorporates recognition of existing regulatory and voluntary reporting requirements that address emergency preparedness and business continuity.**
- **Participants cited a number of existing reporting frameworks, regulations and industry practices that address emergency preparedness and resilience which should be considered in the development and implementation of the certification program.**
- **Reporting and documentation on conformity to relevant existing standards and other guidance should be evaluated for potential recognition by the certification program even if the specific standard may not be a designated core standard of the program.**
- **There is also a potential for the certification program to include recognition of efforts undertaken by firms to report preparedness efforts in the contexts of insurance underwriting, rating agency analysis, supply chain resilience and legal documentation.**
- **Participants discussed the potential value of a comprehensive list of preparedness-related reporting frameworks, regulations, guidelines and practices.**

## **ABOUT THE INTERNATIONAL CENTER FOR ENTERPRISE PREPAREDNESS (InterCEP)**

- InterCEP is the world's first academic research center dedicated to private sector preparedness & resilience.
- The Alfred P. Sloan Foundation funds InterCEP's research on incentives for business preparedness in the following areas:
  - Insurance, rating agency, mitigating legal liability, supply chain, corporate governance.
- InterCEP's research focuses on linking the "what" and the "why" of preparedness and resilience:
  - "What" should be done in terms of preparedness is often most effectively reflected in preparedness standards and best practices.
  - "Why" preparedness efforts should be undertaken by business generally includes both internal economic impacts of preparedness as well as external incentives.
  - Linkage of the "what" and "why" of preparedness often requires measurement or assessment to determine if the "what" to do of preparedness has been accomplished so that the "why" to do it can be achieved or rewarded.

## **MEETING AGENDA**

- 11:00 – 11:10: Overview of New Law: "The Implementing Recommendations of the 9/11 Commission Act of 2007" (Public Law 110-53 – Title IX, Section 524)
- 11:10 – 11:20: Focusing on the rating agency perspective: Key questions
- 11:20 – 12:00: Open, facilitated discussion
- 12:00 – 12:30: Defining the Working Group agenda, including: possible next steps, activities, recommendations, etc.

## **GROUND RULES**

- Participants may contribute directly to the conversation but should be recognized by the moderator first.
- Conference call will be recorded.
- All comments are not-for-attribution.
- Those not participating verbally, please forward your questions and comments throughout the discussion via Question & Answer Function.
- For post-forum comments, please email to [intercep@nyu.edu](mailto:intercep@nyu.edu).

## **OVERVIEW OF NEW LAW**

"The Implementing Recommendations of the 9/11 Commission Act of 2007" (Public Law 110-534) was signed into law on August 3, 2007. Title IX Section 524 of the law calls for the creation of a voluntary business preparedness accreditation and certification program. The legislation stipulates that the program should:

- Provide a method to independently certify the emergency preparedness of private sector organizations, including disaster/emergency management and business continuity programs;
- Be administered outside of government by third party organizations with experience / expertise in managing and implementing voluntary accreditation and certification programs;
- Be voluntary;

- Designate one or more preparedness standards. NFPA 1600 is referenced as an example;
- Integrate/recognize where appropriate existing industry efforts, standards, practices and reporting in this area;
- Give special consideration to small businesses; and
- Protect proprietary and confidential information of companies.

### **U.S. DEPARTMENT OF HOMELAND SECURITY'S RESPONSIBILITIES**

The legislation also assigns the following specific responsibilities to the U.S. Department of Homeland Security (DHS):

- Designate one or more organizations to act as the accrediting body to develop and oversee the certification process, and to accredit qualified third parties to carry out the certification program;
- Separately designate one or more standards for assessing private sector preparedness;
- Provide information and promote the business case for voluntary compliance with preparedness standards; and
- Monitor the effectiveness of program on an ongoing basis.

### **CURRENT STATUS & LIKELY TRAJECTORY**

As of March 28, 2008, the current status and likely trajectory of the certification program development process (to the best of InterCEP's knowledge) reflects the following:

- A 'Framework for Voluntary Preparedness' encompassing multiple preparedness standards and other guidance has been developed by key organizations (RIMS, DRII, ASIS, NFPA) with the support of the Alfred P. Sloan Foundation.<sup>1</sup> This document argues for flexibility within a framework in terms of certification activity potentially including the recognition of multiple preparedness standards/guidance by the program.
- DHS is preparing to report soon to Congress on a plan for program development.
- A potential accreditation body has been identified and notification published. That body is ANAB which has substantial experience in administering the private sector driven and voluntary certification efforts in quality management and environmental management.
- One or more preparedness standards are still to be designated by DHS.
- Outreach to the private sector for input is in process by DHS and includes a National Stakeholder Forum sponsored by the Sloan Foundation and hosted by InterCEP in December 2007.
- Legislation requires stakeholder input and this takes time.
- Pilot projects will likely lead introduction.
- Supply chain "push down" may be factor.
- Certification of small businesses may be addressed separately and later on in the process.

### **THE WORKING GROUPS INITIATIVE**

The objectives of InterCEP's initiative to organize Working Groups focused on the voluntary business preparedness accreditation and certification program are as follows:

- To identify existing practices and principles in specific topical areas relevant to private sector preparedness;

---

<sup>1</sup> Cf. "Framework for Voluntary Preparedness – Briefing Regarding Private Sector Approaches to H.R. 1 and public Law 110-53 'Implementing Recommendations of the 9/11 Commission Act of 2007' Title IX" prepared by representatives of ASIS International, DRII, NFPA, and RIMS. Available at [www.sloan.org](http://www.sloan.org)

- In view of these practices and principles, to identify issues, opportunities and potential strategies relevant to the design and implementation of the voluntary business preparedness certification program that would promote effectiveness and business value of the program; and,
- To gather these outputs generated by Working Group participants and communicate them to program stakeholders including where appropriate DHS, accrediting and certifying bodies.
- To place emphasis on five areas of incentives that, according to InterCEP's ongoing research, could provide economic value to businesses that pursue certification, including: supply chain management, legal liability mitigation, rating agency acknowledgement, insurance and existing business reporting.

## THE BUSINESS REPORTING PERSPECTIVE

InterCEP's ongoing research on incentives for business preparedness has indicated that businesses already operate within a variety of different reporting frameworks, both voluntary and regulatory, that address elements of emergency management and business continuity. With regard to the potential significance of the voluntary business certification program in reference to these existing frameworks, discussion among participants in the initial meeting of the Business Reporting Working Group is framed by the following key questions:

- What existing business reporting requirements (incl., voluntary and regulatory frameworks) address elements of preparedness?
- How should the preparedness certification program be designed and implemented in order to accommodate/acknowledge existing preparedness reporting efforts and avoid any unnecessary duplication?

## DISCUSSION

InterCEP has identified general themes developed during the Working Group discussion. In this summary, these themes are briefly articulated, and then specific issues relevant to each theme are presented. Comments by participants have not been independently confirmed by InterCEP.

- **Participants acknowledged the importance of making sure that the voluntary certification program incorporates recognition of existing regulatory and voluntary reporting requirements that address emergency preparedness and business continuity.**
  - Many businesses already report their efforts to develop and improve business continuity and emergency preparedness capabilities, whether based on regulatory requirements, voluntarily in accordance with existing practices, or in the context of second-party audits that take place between and among supply chain partners.
  - According to the legislation, the voluntary certification program should where appropriate integrate and recognize such ongoing efforts.
- **Participants cited a number of existing reporting frameworks, regulations and industry practices that address emergency preparedness and resilience which should be considered in the development and implementation of the certification program, including the following:**
  - In 2004, the Securities and Exchange Commission (SEC) approved NASD and NYSE rules (File Nos. SR-NASD-2002-108 and SR NYSE-2002-35), that require members to have in place business continuity plans relating to an emergency or significant business disruption. Furthermore, NYSE Regulation and the NASD have merged to form the Financial Industry Regulatory Authority (FINRA), which is currently in the process of merging the two rules into a single rule for all broker-dealers. In addition, the SEC also

- has other rules and interagency papers that set resiliency goals for exchanges, clearing organizations and significant firms handling 5% or more of volume in a critical market.
- The Federal Financial Institutions Examination Council (FFIEC) has developed a Business Continuity Planning Work Program designed to determine the quality and effectiveness of the organization's business continuity planning process, and determine whether the continuity testing program is sufficient to demonstrate the financial institution's ability to meet its continuity objectives. The FFIEC Business Continuity Planning Booklet is one of the twelve booklets that comprise the FFEIC IT Examination Handbook. While the BCP booklet is most frequently considered in reference to the development of preparedness standards, the issue of business continuity and resiliency runs throughout the other eleven booklets as well, which include topics such as: Audit, Management and Operations; Outsourcing Technology Services; Supervision of TSP's; e-Banking, Fed Line, Retail and Wholesale Payment Systems; Development and Acquisition; Information Security; etc. Each and all of these booklets should therefore be considered by financial services firms when addressing issues of preparedness and resiliency.
  - BITS is a not-for-profit, CEO-driven financial service industry consortium made up of 100 of the largest financial institutions in the US. BITS administers the Financial Institution Shared Assessments Program (FISAP), a process for financial institutions to evaluate the security controls of their IT service providers.
  - Within the electrical utilities industry, The U.S. Department of Energy has designated the North American Electric Reliability Corporation (NERC) as the electricity sector coordinator for critical infrastructure protection. NERC's Critical Infrastructure Protection Committee (CIPC) coordinates NERC's initiatives in the areas of cyber security, physical security, and operational security.
  - Administered by the U.S. Federal Communications Commission (FCC), the National Security for Emergency Preparedness (NS/EP) telecommunications program requires telecom firms to provide critical services that are used to maintain a state of readiness. Additionally, telecom firms are required to respond to and manage any event or crisis (local, national, or international) that causes or could cause injury or harm to the population, damage to or loss of property, or degrade or threaten the national security or emergency preparedness posture of the United States.
  - The Joint Commission on the Accreditation of Healthcare Organizations (JCAHO) sets standards for healthcare organizations and issues accreditation to organizations that meet those standards, which include elements of business continuity and emergency preparedness.
  - The Occupational Safety and Health Administration (OSHA), within the U.S. Department of Labor, administers a series of Occupational Safety And Health Standards (1910) that bear upon emergency preparedness, including requirements for business to have emergency action plans, to control dangerous work conditions and hazardous substances, etc.
  - Administered by the U.S. Customs Service, The Customs-Trade Partnership Against Terrorism (C-TPAT) is a joint government-business initiative to build cooperative relationships that strengthen overall supply chain and border security by ensuring the integrity of their security practices and communicating their security guidelines to their business partners within the supply chain.
  - Any business which stores, uses, or releases hazardous materials may be required to comply with one or more provision of The Superfund Amendments and Reauthorization Act (SARA) Title III, known as the Emergency Planning and Community Right to Know Act, (40 CFR 300-355). This legislation establishes the public's right to know what chemicals are stored in their communities and requires state and local governments to establish local committees to identify hazardous materials and to plan for responding to releases of the materials.
  - Administered by the U.S. Department of Homeland Security (DHS), the Chemical Facility Anti-Terrorism Standards (CFATS) requires firms in the chemical industry to conduct a security vulnerability assessment (SVA) and then develop and implement a Site Security

- Plan (SSP) plan implementing security measures that meet Risk Based Performance Standards (RBPS).
- The State Of New York Insurance Department has issued a series of Circular Letters (e.g., Circular Letter No. 1 (2008)) that require insurance companies to report on their own disaster response plans, especially as these plans are necessary to maintain the effectiveness and accuracy of information used by the NYS Disaster Coalition in the event of a future disaster.
  - Administered within the U.S. Department of Health and Human Services (HHS), the Health Insurance Portability and Accountability Act of 1996 (HIPAA) includes a Security Rule 164.308(a)(7) that requires firms that handle health-related information to have administrative safeguards including contingency plans, disaster recovery plans, and data backup plans; physical safeguards including access controls and contingency operations; and technical safeguards including emergency access procedures.
  - Maturity models (including those developed by the Financial Services Technology Consortium (FSTC) and the Virtual Corporation) provide a means of differentiating levels of proficiency in practice, and allow for management decision-making about how to improve practice over time. For example, a non-critical business unit may require only Level 1 maturity for its business continuity program, while a critical unit involving hazardous materials may require the highest Level 5 maturity. While not regulatory or reporting requirements per se, maturity models could potentially be considered by the certification program in some regard.
  - Environmental reporting requirements may additionally be considered where appropriate.
- **Reporting and documentation on conformity to relevant existing standards and other guidance should be evaluated for potential recognition by the certification program even if the specific standard may not be a designated core standard of the program.**
    - Examples of potentially relevant standards were identified by representatives from RIMS, ASIS, NFPA and DRII, who worked together on an initiative sponsored by the Alfred P. Sloan Foundation to develop a “Framework for Voluntary Preparedness.”<sup>2</sup> The document provides a crosswalk that emphasizes the commonalities that exist between a number of existing standards and other guidance, including:
      - NFPA 1600: 2007 – Standard on Disaster/Emergency Management and Business Continuity Programs
      - BS 25999-2: 2007 – Business Continuity Management – Part 2: Specification
      - CSA Z1600: Standard on Emergency Management and Business Continuity Programs
      - TR19: 2005 – Technical Reference for Business Continuity Management (BCM)
      - ISO Publicly Available Specification (PAS) 22399: 2007 – Societal Security: Guidelines for Incident Preparedness and Operational Continuity Management.
      - ASIS International – Organizational Resilience: Preparedness and Continuity Management Best Practices Standard.
      - DRI/BCI – Professional Practices for Business Continuity Planners.
    - Working group participants also referenced yet another preparedness standard from Singapore, SS507: 2004, which covers business continuity/disaster recovery (BC/DR) service providers.
  - **There is also a potential for the certification program to include recognition of efforts undertaken by firms to report preparedness efforts in the contexts of insurance underwriting, rating agency analysis, supply chain resilience and legal documentation.**
    - The primary orientation of InterCEP’s other four Working Groups (Insurance, Legal, Supply Chain and Rating Agency) is to explore how the certification program might be designed to provide information relevant to the development of business incentives in each of these areas. However, it is relevant to consider how, conversely, existing efforts in those areas may be taken as inputs to the certification process. Just as existing

---

<sup>2</sup> Op cit.

reporting efforts may need to be integrated into the certification audit process, so too existing efforts to present evidence of preparedness to underwriters, lawyers, ratings analysts, and second-party auditors in supply chain relationships may also be integrated.

- **Participants discussed the potential value of a comprehensive list of preparedness-related reporting frameworks and regulations, guidelines and practices.**

### **INTERCEP'S ACTIVITIES**

InterCEP is committed to supporting the Business Reporting Working Group by undertaking the following activities:

- Produce high-level summary proceedings of Working Group meetings, to be drafted by InterCEP, then vetted with participants, and finally distributed for stakeholder consideration;
- Develop greater awareness within the general business community of the voluntary business preparedness certification program;
- Produce research output that presents knowledge generated by the working group relevant to the design and implementation of the voluntary business preparedness accreditation and certification program;
- Develop an online clearinghouse of documentation relevant to the voluntary business preparedness accreditation and certification program.

### **SETTING THE WORKING GROUP AGENDA MOVING FORWARD**

Next steps possibly to be undertaken by InterCEP with the support and involvement of members of the Business Reporting Working Group include:

- Develop a comprehensive list of relevant, existing reporting requirements, regulations and industry activities etc. that address emergency preparedness that could be potentially credited or otherwise integrated into the certification program. Key components of this next step may include:
  - Reaching out to sector-specific industry/trade associations to identify relevant reporting and regulatory practices.
  - Reaching out to DHS critical infrastructure sector coordinating councils.
  - Reaching out to all relevant discipline-specific professional associations (e.g., ASIS, RIMS, IAEM, ISMA, DRII, ACP, NEMA, etc.) as a way to inform and mobilize their members.
  - Reaching out to regional public-private partnerships and other associations of risk-oriented professionals (e.g., the Great Lakes Business Recovery Group (GLBRG), Chicago First, Business Executives for National Security (BENS), Contingency Planning and Recovery Management (CPARM), the Southeast Business Recovery Exchange (SEBRE), the Contingency Planning Association of the Carolinas (CPAC), Business Continuity Professionals of the Carolinas (BCPC) etc.)
- Relate this list to the designated standard(s) of the certification program and/or alternatively to the set of common preparedness elements identified in the Sloan Framework for Voluntary Preparedness.
- Develop a recommendation for a methodology to credit conformity with components of this list in receiving certification under the program.
- Provide information, findings and recommendations as appropriate to the U.S. Department of Homeland Security and the designated accrediting body. Note that ANAB has been provisionally designated as the accrediting body and InterCEP Director Bill Raisch has been appointed to the ANAB Committee of Experts for the Voluntary Private Sector Preparedness Certification Program.

With respect to each of these possible next steps, InterCEP seeks feedback and indications of interest from Working Group participants and readers of this document in response to the following questions:

- Do you think these next steps would have value?
- Do you have any information relevant to these next steps?
- Would you like to get involved and help craft these next steps?

In general, InterCEP is committed to facilitating the agenda for the Working Group, including additional next steps and other action items, based on the feedback gathered from participants in response to these additional questions:

- Who else should be at this table?
- In what forums should this discussion be taking place?
- Who/what are the most relevant individuals, job titles, organizations, associations, etc.?
- What concrete next steps can be taken to acknowledge, integrate, and credit existing efforts?
- Additional next steps – what are we missing?
- What meeting formats are most appropriate to maximize participation and productivity?
- How regularly should Working Group meetings be scheduled?

InterCEP encourages readers of this document and other stakeholders to contact us on an ongoing basis with questions, comments and suggestions regarding the Working Group agenda, as well as in reference to the broader process of developing and implementing the certification program. InterCEP's efforts to support this process are undertaken independent of any government agency or accrediting body with the financial support of the Alfred P. Sloan Foundation.

*International Center for Enterprise Preparedness, New York University (NYU)*  
113 University Place, 9<sup>th</sup> Floor, New York, NY 10003  
+ 1- 212-998-2000 (t) + 1-212-995-4614 (f)