

Are You Ready?

Private Sector Standards & Certification

Title IX, Private Sector Preparedness Act (PL 110-53)

- Implemented recommendations of 9/11 Commission (HR 1)
- Enacted August 3, 2007; effective December 9, 2007
- Within 210 days, DHS will:
 - Adopt one or more **standards** for private sector business preparedness
 - ✓ Designate one or more organizations (**accrediting body**) to:
 - Develop and oversee the certification process
 - Accredit third parties (**certifying bodies**) to implement the certification program
 - ✓ ANSI National Accreditation Board (ANAB) designated
 - Provide information and **promote “voluntary” compliance** with standard(s)
 - **Monitor effectiveness** of program on recurring basis
- Mandates “all hazards” approach, industry-specific “best practices” and differentiation between large/small businesses

Title IX, Private Sector Preparedness Act ***(PL 110-53)***

LEGISLATIVE STIPULATIONS

- ➔ **Independent certification** of private sector emergency preparedness (including disaster/emergency management & business continuity)
- ➔ Administer **outside government** by third parties
- ➔ Give special consideration to **small businesses** (15 USC 632)
- ➔ Protect **proprietary/confidential** company information & data
- ➔ Consist of **one or more standards** (NFPA 1600 cited)
- ➔ Integrate, recognize & credit **existing industry efforts**, standards, best practices and reporting
- ➔ Be **voluntary**

Key Terms

- Regulation
 - Official document, force of law (e.g. SOX)
- Standard
 - Consensus document, industry best practices
- Conformity Assessment (Audit)
 - Internal (first party)
 - Customer/supplier (second party)
 - Independent organization (third party)
- Accrediting Body (Accreditation)
 - ANSI National Accreditation Board (ANAB)
- Certifying Body (Certification)
 - Assessor or auditor
- Approving Body (Adoption)
 - DHS PS-Prep Coordinating Council (PSPCC)

NFPA 1600 – Current US Standard

- 1991 Technical Committee on Disaster Management formed
- 1995 Recommended Practice for Disaster Management
- 2000 Standard on Disaster/Emergency Management and Business Continuity Programs – 1st Ed.
- 2004 2nd Edition published
- 2007 3rd Edition published
- 2010 4th Edition scheduled



Freely available at: <http://www.nfpa.org/assets/files/PDF/NFPA1600.pdf>

Preparedness Standards & Best Practices

Standard	Developing Organization	Original Date of Release	Revision Cycle	Composition of Technical Committee
NFPA 1600:2007 Standard on Disaster / Emergency Management & Business Continuity	National Fire Protection Association (NFPA)	1991	Revised in 1995, 2004, & 2007	53 members, alternates and nonvoting members, including representatives of a range of public and private sector organizations.
ISO/PAS 22399:2007 Incident Preparedness & Organizational Continuity	International Standards Organization (ISO)	2007		46 members, including 12 members from developing countries
ASIS International All-Hazards	ASIS International		Draft presented for comment, 2007; currently under revision	168 members including representatives of the private sector and academic organizations
BS 25999-2: 2007	British Standards Institution (BSI)	2007		40 full members, including consultants and users from a range of public and private sector organizations

Preparedness Standards & Best Practices

Standard	Developing Organization	Original Date of Release	Revision Cycle	Composition of Technical Committee
CSA Z1600	Canadian Standards Association (CSA)	Under enquiry stage (public & internal review)		Cross-sector full and associate (non-voting) members from business, industry, and the public sector
TR19: 2005	Singapore SPRING (Standards, Productivity and Innovation Board)	2005		Some 70 volunteer members of key industry and government sectors with consultation with Singapore Business Federation (SBF)
DRII/ BCI Prof. Practices	Disaster Recovery Institute International/ Business Continuity Institute (BCI)	2003	2004 (2 nd Edition)	Range of professionals from DRII, BCI, and other emergency management professional associations

Other Regulatory Drivers

Sarbanes-Oxley (SOX)

- ➔ Financial accountability & disclosure

Health Insurance Portability & Accountability Act (HIPPA)

- ➔ Document protection & control

Graham-Leach-Bliley Act

- ➔ Protection & privacy of financial information

Occupational Safety & Health Administration (OSHA)

- ➔ Life & fire safety

Federal Financial Institutions Examination Council (FFIEC)

- ➔ Continuity of business operations

Homeland Security Act (DHS)

- ➔ Critical infrastructure security & protection

North American Electric Reliability Corporation (NERC)

- ➔ Utility availability & security protection

Chemical Facilities Anti-Terrorism Standards (CFATS)

- ➔ Chemical storage & security protection

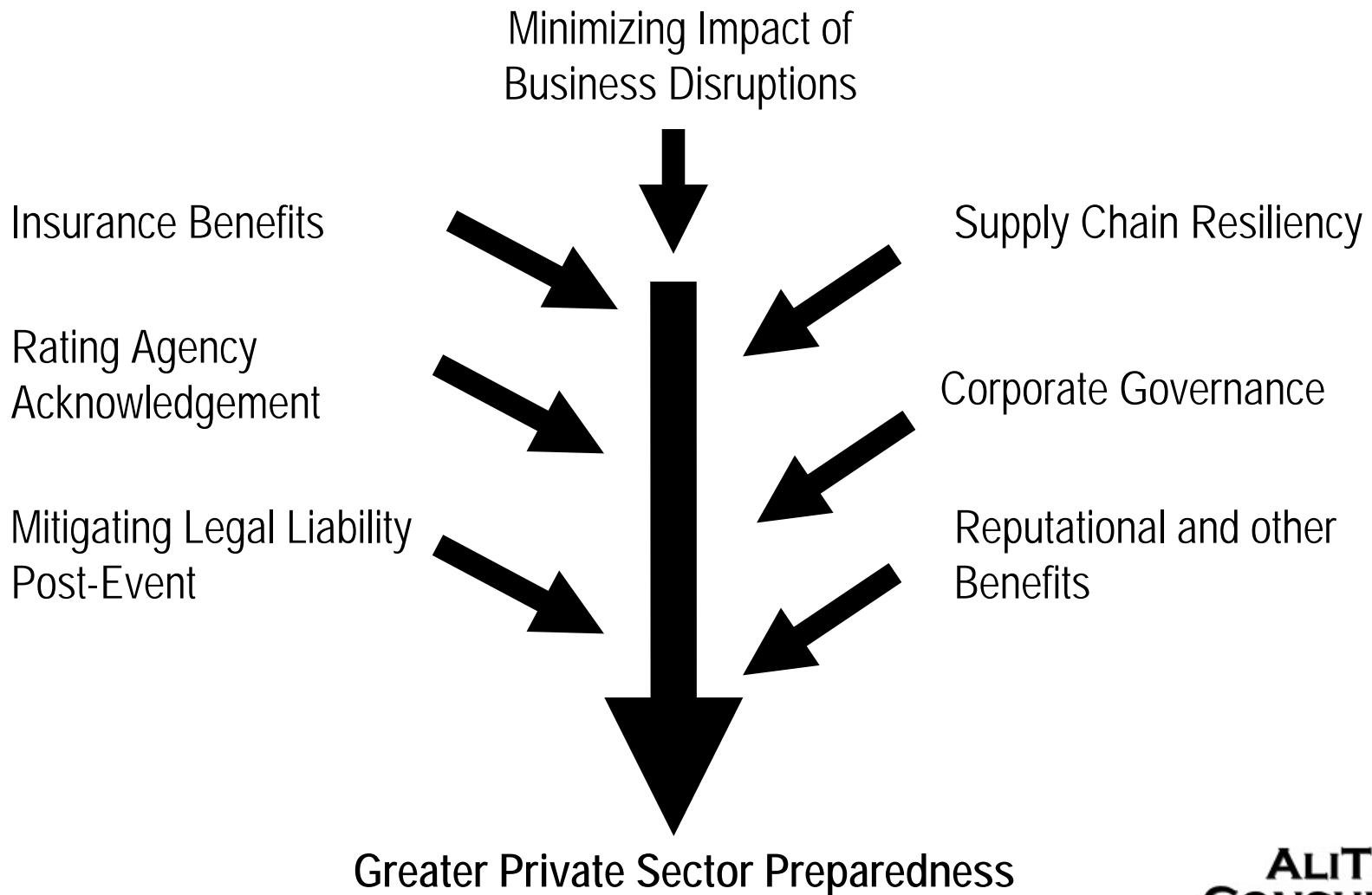
Common Requirements (80+% Similar)

1. Policy statement
2. Management commitment
3. Risk identification, assessment & analysis
4. Protect proprietary & confidential information
5. Incident management procedures & controls
6. Data control & backup (documents & information)
7. Continuity of critical operations
8. Exercises & testing
9. Independent audits

Potential Benefits of Title IX

- ➔ **Preparedness**
 - ➔ Private sector more resilient
- ➔ **Compliance**
 - ➔ Avoid consequences & sanctions
- ➔ **Minimize legal liability**
 - ➔ “Safe harbor”, legal standard of care
- ➔ **Reduced insurance costs**
 - ➔ Resiliency = lower exposure/risk
- ➔ **Improved credit ratings**
 - ➔ Greater risk capacity = more financial stability
- ➔ **Supply chain enhancements**
 - ➔ Increased vendor dependability, ease in auditing
- ➔ **Market differentiation**
 - ➔ Improved efficiency, effectiveness & agility

Value in Title IX Standards



Likely Title IX Certification Steps

1. Review of your current state of emergency preparedness against selected standard (gap analysis)
2. Supplement and/or improve your existing preparedness processes, plans & activities to meet intent of desired standard(s)
3. Contract with accredited certification body for assessment and certification
4. On-going surveillance and continual improvement processes

Current Status of Title IX

- ➔ ASIS, NFPA, RIMS and DRII wrote “**framework report**”
- ➔ **InterCEP/Sloan Foundation** conducting supporting research (available @ <http://www.nyu.edu/intercep>)
 - ➔ Working groups (legal, supply chain, insurance, credit rating)
 - ➔ Publications clearinghouse
 - ➔ Target sector articles & meetings
- ➔ DHS **posted Federal Register Notice** on program planning; draft criteria & potential standards out for public comment
- ➔ **ANAB under contract** as Title IX accrediting body
- ➔ **Public meetings scheduled** (January-February 2009)
- ➔ One or more **standards still to be designated**; NIPP sectors will have major role

Current Status of Title IX

- ➔ Now officially designated “**PS-Prep**”
- ➔ **FEMA Administrator** is responsible
 - ➔ PS-Prep Coordinating Council (**PSPCC**) established
- ➔ Communications & comments through
 - ➔ CIKR Sector Coordinating Councils (**SCCs**)
 - ➔ Public **meetings**, rulemaking **website** (www.regulations.gov)
- ➔ DHS is encouraging **multiple standards**
 - ➔ General, broad-based (**first**)
 - ➔ Limited, industry-specific (**later**)
 - ➔ **All groups** can develop/propose standards, not just SDOs
 - ➔ **One or more categories** (preparedness, business continuity, disaster or emergency management)
- ➔ Initial certifications will be “**conformity or non-conformity**” based
- ➔ Certification data may be classified “**PCII Sensitive**”

Sloan Foundation Framework Report

➤ Key points:

- In order 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 their needs
- Report identifies core common elements of a preparedness program and provides a **crosswalk of existing standards**, guidelines and best practices
- Businesses and organizations should be afforded the flexibility to **build on their existing programs**
- Small businesses in particular need to tailor their preparedness and resilience strategies to their **financial realities**
- A major barrier to preparedness and resilience management is a **lack of knowledge and tools**, particularly in the case of small businesses

Standard or Regulation?

- ➔ **Voluntary consensus** standards are written in an open environment by professionals from both the private and the public sectors
- ➔ Developed by people **experienced** in the field
- ➔ Represent the **best and brightest thinking** in the area
- ➔ **Alternative** to government regulations in many areas
- ➔ Makes possible applications, communications and connection **compatibility**
- ➔ **Levels the playing field** and assures fair competition by requiring all suppliers to meet a common set of requirements

Potential Benefits of a Compliance Assessment Program

- Can facilitate the **acknowledgement and rewarding** of preparedness efforts (insurance, legal, rating agency, etc.)
- May facilitate exchange of **best practices**
- Enables more consistent **benchmarking** internally and externally
- May facilitate **financial analysis**
- May advance corporate **governance goals**
- Would increase **business preparedness**

Current ASIS Standards Initiative

ANSI Authorized Standards Development Organization (SDO)

- Announced July 30, 2008
- Rigidly following prescribed ANSI standards development process
 - Inclusive process; open invitation
 - Not weighted toward physical security or ASIS
- Stakeholders meeting held October 3, 2008
 - Recognized conflict with NFPA 1600
 - Endorsed "compelling need" to develop new standard

Focused on Management vs. Technical Standard

- Will use BS 25999 as starting point
 - Management focus, only currently auditable BCM standard
- Close coordination & alignment with key standards organizations
 - US-based ANSI National Accreditation Board (ANAB)
 - Geneva-based Organization for Standardization (ISO)

Serve Multiple Functions

- Title IX Acceptable
- Accredited by ANSI as US business continuity standard
- Partnerships with ISO, BSI and Dutch as new international BC standard

Improve Existing Shortfalls

- 1st, 2nd and 3rd Party Certifications
- Maturity Model/Levels

Status

- ACP represented on both Technical Committee and Working Group
 - Initial organizing meeting on December 8, 2008
 - First working session on January 15-16, 2009

Current Unresolved Issues

Which Standards?

- ➔ NFPA 1600 – previous US business continuity standard
- ➔ BS 25999 – more recent, comprehensive British proposal
- ➔ ISO/PAS 22399 – covers international/global operations
- ➔ New ASIS Effort – focus on management systems
- ➔ New Industry-specific efforts
- ➔ 80+% of requirements are similar

What Accrediting Body?

- ➔ US-based ANSI National Accreditation Board (ANAB)
- ➔ Geneva-based Organization for Standardization (ISO)

Who Certifies?

- ➔ 1st Party (self)
- ➔ 2nd Party (customer, vendor)
- ➔ 3rd Party (external audit, certifying body)

When Needed?

- ➔ Milestones missed, decisions delayed
- ➔ Change in administration

How Extensive – business size, criticality?

ACP Special Committee & Focus Areas

- Michelle Cross (Chairperson)
- Don Byrne (Accreditation)
 - ANAB Committee of Experts
- Doug Moore
- Susan Mitchell
- Phil Oppenheim (Conferences)
 - CPM West
- Mike Thomson (Standards)
 - ASIS Technical Committee/New BC Standard

Questions

