PS-Prep: Voluntary Private Sector Preparedness Program

Chemical Summit
July 6, 2011

Tracy Shawyer
Partnership and Outreach Division
Office of Infrastructure Protection
Implementing Recommendations of the 9/11 Commission Act of 2007 (Public Law 110-53)

Mandated Action

- Directs DHS to establish a “Voluntary Private Sector Preparedness Accreditation and Certification Program”
- Select preparedness standards and establish accreditation and certification program

Improve Private Sector Preparedness in:

- Disaster management
- Emergency management
- Business continuity

Key Program Requirements

- Voluntary Participation
- Provide a method to independently certify preparedness of private-sector entities (third-party certification)
- Integrate and leverage existing regulatory requirements and programs, if feasible
Adopted Standards

On June 15, 2010, DHS announced adoption of the following standards:

- **NFPA 1600** - Standard on Disaster / Emergency Management and Business Continuity Programs, “...a common set of criteria for preparedness, disaster management, emergency management, and business continuity.” (2007 and 2010 editions)

- **BS 25999** - Business Continuity Management, “...defines requirements for a management systems approach to business continuity, and integrates risk management disciplines and processes.”

Certification Program Model

Certification

- Third-party certification, with self-declaration of conformity option for small businesses.
- Third-party certification can be obtained only from an accredited certifying body.

Certification Process

- Certification involves document reviews, site visits, and audits.
- May involve the full range of organizational activities that are applicable to the desired certification.
A Comprehensive Preparedness Program

1. Program Policies and Management
Top-level authorization, support, and commitment should be given to the preparedness program. An organization should take the following actions:
- Develop policy, vision, and mission statements;
- Devote appropriate personnel and financial resources; and
- Assign an individual (or committee, in larger organizations) with appropriate authority to lead the preparedness efforts.

2. Analysis
The following activities are critical for the organization to develop appropriate program goals related to (1) incident prevention and mitigation and (2) incident management and continuity:
- Evaluate legal, statutory, regulatory, and industry best practices, as well as other requirements;
- Define and document the scope of the preparedness program; and
- Conduct a risk assessment and impact analysis.

3. Planning
The organization should develop multiple plans, each of which should have clearly defined end products, a specific schedule, and assigned responsibilities and resources. Primary plans should exist for the following activities:
- Prevention and mitigation; and
- Incident management.
And supporting plans should exist for the following activities:
- Resource management and logistics;
- Training;
- Testing and evaluation; and
- Records management.

4. Implementation
Successful implementation of preparedness programs requires the development and maintenance of a comprehensive project management and control system, which includes the following:
- Each of the specified projects carried out according to the plan, adhering to completion dates;
- Assurance of program-level coordination; and
- Periodic program reviews and internal audits.

5. Testing and Evaluation
For the purpose of quality control, a testing and evaluation plan should incorporate the following elements:
- Specify a series of evaluations to examine various elements of the implementation process;
- Use dry runs to evaluate the program overall; and
- Review findings from these processes to revise plans as needed.

6. Maintenance, Review, and Improvement
The preparedness program requires routine maintenance, review, feedback, and continuous improvements. Programs can achieve these goals by taking the following actions:
- Implementing periodic formal reviews to verify adherence to program requirements and discover areas of improvement;
- Using any available post-incident evaluations, such as special analyses and reports, lessons learned, and performance evaluations; and
- Identifying program areas that require periodic maintenance, and regularly scheduling that maintenance.
The Case For Preparedness

Why prepare?
- Resilience
- Continuity
- Sustainability

Why prepare to a standard?
- Standards developed by groups of external preparedness experts
- Systematic approach - avoid unintentional gaps
- Facilitates appropriate allocation of resources

Why certify?
- Credibility
- Validation of excellence
- Benchmark
  - Corporate, community, citizen
DHS Office of Infrastructure Protection is collaborating with sectors to:

- **Identify** guidelines, best practices, relevant regulations and agreed codes of practice that already apply to the sector
- **Cross-map** to adopted standards
- **Develop framework guide for use** by sector entities as well as certifying bodies in applying standards

**18 Critical Infrastructure Sectors**
- Agriculture and Food
- Defense Industrial Base
- Energy
- Healthcare and Public Health
- National Monuments and Icons
- Banking and Finance
- Water
- Chemical
- Commercial Facilities
- Critical Manufacturing
- Dams
- Emergency Services
- Nuclear Reactors, Materials, and Waste
- Information Technology
- Communications
- Postal and Shipping
- Transportation Systems
- Government Facilities
1. **Introduction** - Provides an overview of the PS-Prep program and the components of the guide.

2. **Getting Prepared** - Details key subject areas of a comprehensive preparedness program.

3. **Getting Certified** - Defines the certification process, description of standards and potential value of certification.

4. **The Sector Perspective** - Describes regulatory landscape, business case for preparedness and considerations prior to certification.
PS-Prep Data Set

- Sector-specific list of preparedness programs, regulations, etc.
- Collected through open source research and contributions by sector partners.
# PS-Prep Data Set

<table>
<thead>
<tr>
<th>TOPIC</th>
<th>ENTITY</th>
<th>TITLE</th>
<th>DESCRIPTION</th>
<th>SOURCE</th>
</tr>
</thead>
<tbody>
<tr>
<td>AUS</td>
<td>ANS I-25-SHPD 2007</td>
<td>Nuclear Critical Accident Emergency Planning and Response</td>
<td>Provides guidance for minimizing risks to personnel during emergency responses to a nuclear criticality accident and includes reactions, applications for facilities where a criticality accident is possible. Does not apply to nuclear power plants that are protected by other standards. Does not apply to facilities that are exposed to radiological injury or radiation.</td>
<td><a href="http://www.ans.org/store/c2007850889116996/">http://www.ans.org/store/c2007850889116996/</a></td>
</tr>
<tr>
<td>AUS</td>
<td>ANS I-3 4.1 WF 2003</td>
<td>Critical Accident Alarm System</td>
<td>Applies to all operations involving hazardous materials that could result in a criticality accident and cause personnel to receive unacceptable exposure to radiation.</td>
<td><a href="http://www.ans.org/store/c2007850889116996/">http://www.ans.org/store/c2007850889116996/</a></td>
</tr>
<tr>
<td>DHS</td>
<td>DHS</td>
<td>Protective Action Guide for Radiological Dispersal Device (RDD) and Nuclear Device (NDD) Incidents</td>
<td>This guidance recommends &quot;protective action guides&quot; (PAGs) to support decisions about actions that may need to be taken to protect the public when responding to or recovering from an RDD or NDD incident. Also addresses the implementation of the recommendations and FAQs.</td>
<td><a href="http://www.fema.gov/pdf/about/divisions/fpd/rpgs_4.pdf">http://www.fema.gov/pdf/about/divisions/fpd/rpgs_4.pdf</a></td>
</tr>
<tr>
<td>EPR</td>
<td>Energy Policy Act of 2005</td>
<td>Among other activities, Section 511(a) requires establishment of an interagency task force to report to the President and Congress on the security of nuclear sources in the U.S. from potential thefts, to develop recommendations for regulatory and legislative changes related to protection and security of sources.</td>
<td><a href="http://www.nsa.gov/about-nsa/">http://www.nsa.gov/about-nsa/</a></td>
<td></td>
</tr>
</tbody>
</table>
Worksheets may be used to assist in performing a preliminary self-assessment for voluntary certification after defining scope

**Step 1:** Know the preparedness standard

**Step 2:** Review internal preparedness practices

**Step 3:** Align existing preparedness practices as closely as possible to individual elements of chosen standard
## PS-Prep Mapping Guide

<table>
<thead>
<tr>
<th>Key Subject Areas</th>
<th>NFPA 1600</th>
<th>BS 25999-2</th>
<th>ASIS SPC.1</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Program Policies and Management</td>
<td>4.1/4.2/4.3/4.4</td>
<td>3.1/3.2.2/3.2.3/3.2.4/3.3</td>
<td>4.1.1/4.2.1/4.2.2/4.4.1</td>
</tr>
<tr>
<td>2. Analysis</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>A. Scope</td>
<td>4.5</td>
<td>3.2.1</td>
<td>4.1.1</td>
</tr>
<tr>
<td>B. Risk Assessment</td>
<td>5.4</td>
<td>4.1.2</td>
<td>4.3.1/4.3.2</td>
</tr>
<tr>
<td>C. Impact Analysis</td>
<td>5.5</td>
<td>4.1.1</td>
<td>4.3.1</td>
</tr>
<tr>
<td>D. Establish Goals</td>
<td>4.6</td>
<td>4.1.3/4.2</td>
<td>4.3.3</td>
</tr>
<tr>
<td>3. Planning / 4. Implementation</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>A. Prevention/Mitigation</td>
<td>5.1-5.3/5.6/5.7</td>
<td>4.1.3</td>
<td>4.4.7</td>
</tr>
<tr>
<td>B. Incident Management – Response</td>
<td>5.1-5.3/6.4 6.6/6.9</td>
<td>4.3</td>
<td>4.4.6/4.4.7</td>
</tr>
<tr>
<td>C. Incident Management – Continuity</td>
<td>6.4/6.7/6.9</td>
<td>4.3</td>
<td>4.4.6/4.4.7</td>
</tr>
<tr>
<td>D. Incident Management – Recovery</td>
<td>6.4/6.7/6.9</td>
<td>4.3</td>
<td>4.4.6/4.4.7</td>
</tr>
<tr>
<td>E. Incident Management – Communications and Warning</td>
<td>6.3</td>
<td>4.3</td>
<td>4.4.3/4.4.7</td>
</tr>
<tr>
<td>F. Incident Management – Facilities</td>
<td>6.10</td>
<td>4.3</td>
<td>4.4.7</td>
</tr>
<tr>
<td>G. Incident Management – Crisis Communications and Public Information</td>
<td>6.8</td>
<td>4.3</td>
<td>4.4.7</td>
</tr>
<tr>
<td>H. Incident Management – Finance and Administration</td>
<td>4.7</td>
<td>4.3</td>
<td>4.4.7</td>
</tr>
<tr>
<td>I. Resource Management and Logistics</td>
<td>4.8/6.1</td>
<td>4.3</td>
<td>4.4.1</td>
</tr>
<tr>
<td>J. Training</td>
<td>6.11</td>
<td>3.2.4/3.3</td>
<td>4.4.2</td>
</tr>
<tr>
<td>K. Records Management/Reporting</td>
<td>4.8</td>
<td>3.4/4.3</td>
<td>4.4.4/4.4.5/4.5.4</td>
</tr>
<tr>
<td>5. Test and Evaluation</td>
<td>7</td>
<td>4.4.1/4.4.2</td>
<td>4.5</td>
</tr>
<tr>
<td>6. Maintenance, Review, and Improvement</td>
<td>8</td>
<td>4.4.3/5.1/5.2/6.1/6.2</td>
<td>4.5/4.6</td>
</tr>
</tbody>
</table>
Benefits of Preparedness and Incentives to Certify

- Mitigation of loss of life or injury
- Business survival
- Minimizing impact of business disruptions
- Improved supply chain resilience
- Satisfying customer business continuity requirements
- Improved internal processes
- Improved employee relations
- Improved external relationships
- Satisfy customer, shareholder, and stakeholder expectations
- Potential advantage over unprepared competition
- Lower operating expenses
- Protection of brand and reputation
- Possible insurance industry recognition
- Rating agency acknowledgement
Additional Information

- PS-Prep Resource Center
  [www.fema.gov/privatesector/preparedness](http://www.fema.gov/privatesector/preparedness)
    - Managed by FEMA
    - Links to Three Standards
    - Federal Register Notices
    - Press Releases and Fact Sheets

- Critical Infrastructure Learning Series
  [www.dhs.gov/ciwebinars](http://www.dhs.gov/ciwebinars)
    - Partnering for Critical Infrastructure Preparedness
    - Voluntary Preparedness Standards

- ANAB Web site
  [www.anab.org](http://www.anab.org)
    - Information for certifying bodies
    - Information for entities interested in certification
PS-Prep
Consideration Checklist

Considerations Before Pursuing Certification

Initial Review ✓
- Define the scope of voluntary certification
- Determine which preparedness standard is most appropriate
- Forecast the allocation of internal resources required
- Seek executive sponsorship
- Organize an internal working team of experts

Internal Analysis ✓
- Cross-reference your chosen preparedness standard with internal programs, policies, best practices and existing regulations that will be relevant to certification
- Gather supporting documentation
- Complete a self-assessment with your internal working team of experts
- Brief the executive sponsor on the results of the self-assessment
- Develop a project plan and timeline to close any gaps discovered through self-assessment, bringing your entity closer to compliance with the chosen standard

Certification ✓
- Research, interview and select accredited third party certifiers
- Review your scope, selection of preparedness standard and process of self-assessment with the certifier
- Discuss cost and timeline for completion of certification process
- Brief the executive sponsor and internal working team of experts on all aspects of the certification process
- Complete certification
For more information visit:
www.dhs.gov/criticalinfrastructure

Tracy Shawyer
Director, Partnership and Outreach Division
Tracy.Shawyer@dhs.gov