

PS-Prep: Voluntary Private Sector Preparedness Program

*Chemical Summit
July 6, 2011*



**Homeland
Security**

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



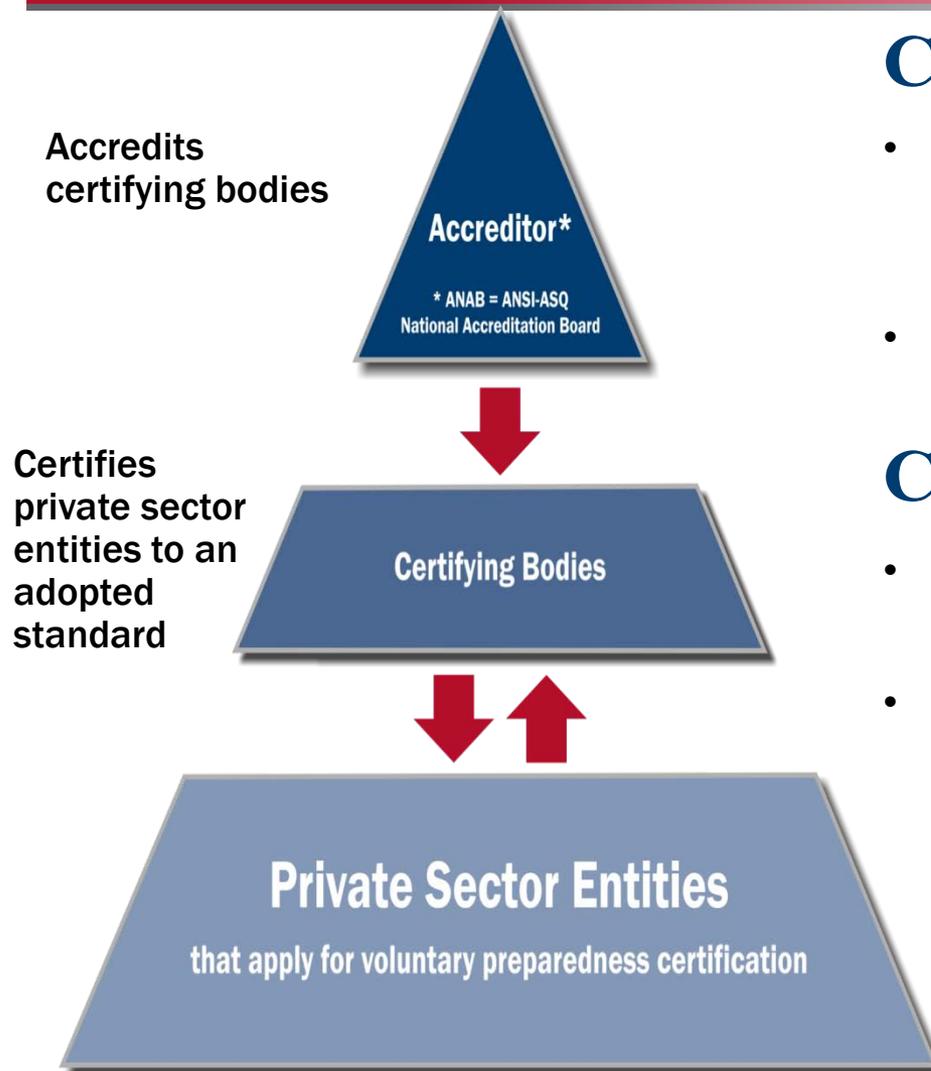
Adopted Standards

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.”
- ***ASIS SPC.1-2009*** - Organizational Resilience: Security, Preparedness, and Continuity Management Systems, “...defines requirements for a management systems approach to organizational resilience.”



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



Critical Infrastructure Sector-Specific Engagements

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

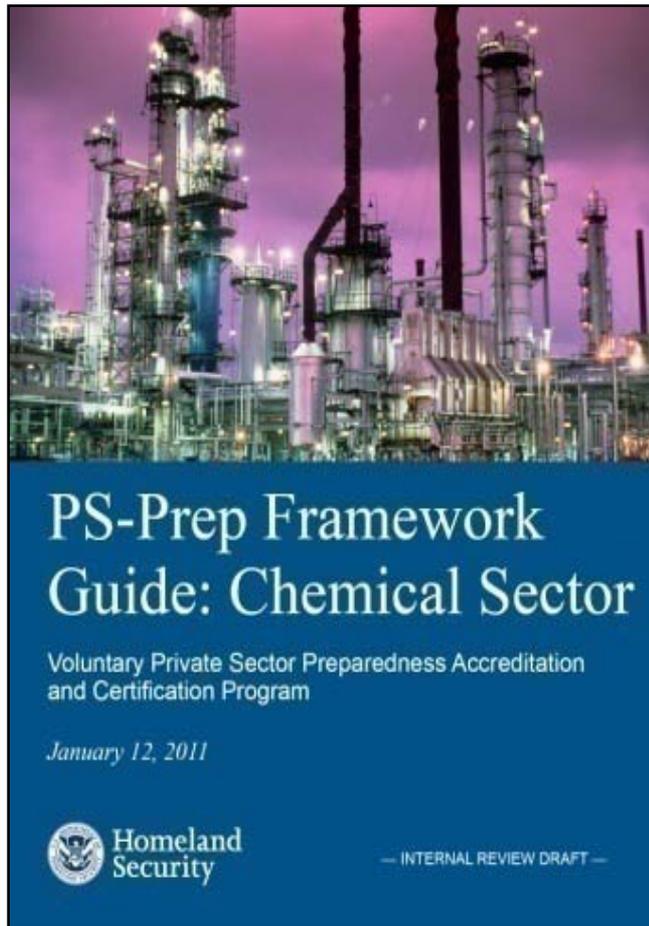
18 Critical Infrastructure Sectors

- 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



PS-Prep

Critical Infrastructure Framework Guide



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

PS-Prep XX Sector Data Set

TOPIC	ENTITY	TITLE	DESCRIPTION	SOURCE
	ANS	ANS-8.23-1997: W2007: Nuclear Criticality Accident Emergency Planning and Response	Provides guidance for minimizing risks to personnel during emergency response to a nuclear criticality accident outside reactors. Applies to facilities for which a criticality accident alarm system is in use. Does not apply to nuclear power plant sites that are addressed by other standards. Does not apply to off-site accidents nor to off-site emergency planning and response.	http://www.new.ans.org/store/L_240228/r_e
	ANS	ANS-8.3-1997: R2003: Criticality Accident Alarm System	Applicable to all operations involving fissionable materials in which inadvertent criticality can occur and cause personnel to receive unacceptable exposure to radiation.	http://www.new.ans.org/store/L_240224
	DHS	DHS Protective Action Guides for Radiological Dispersal Device (RDD) and Improvised Nuclear Device (IND) Incidents	This guidance recommends "protective action guides" (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 IND incident. Also outlines the implementation of the recommendations and the PAGs.	http://www.fema.gov/pdf/about/divisions/thd/repp_rdd_pag.pdf
	DHS	Homeland Security Presidential Directive (HSPD-7) # 7	Established a policy for Federal departments and agencies to identify and prioritize US CIKR to protect them from terrorist attack. The Secretary of DHS will work with the NRC and DOE to ensure protection of Nuclear Sector assets including: identifying, prioritizing, and coordinating protection of CIKR; and facilitating information sharing about physical and cyber threats, vulnerabilities, incidents, potential protective measures, and best practices.	http://www.whitehouse.gov/sites/default/files/omb/assets/omb/memoranda/fy04/m-04-15.pdf
	DHS	Homeland Security Presidential Directive (HSPD-14) #14	Established the Domestic Nuclear Detection Office (DNDO) within DHS to develop, acquire, and support deployment of an enhanced domestic system to detect and report attempts to import, possess, store, transport, develop, or use an unauthorized nuclear explosive device, fissile material, or radioactive material in the U.S.; to improve that system over time; to enhance and coordinate nuclear detection efforts of Federal, State, Territorial, local, and tribal governments and the private sector to ensure a managed, coordinated response.	http://www.dhs.gov/xoig/assets/mgmt/rpts/OIG_08-19_Dec07.pdf
	DOD	National Defense Authorization Act of 2000	Established the National Nuclear Security Administration (NNSA) as a semi-autonomous agency within DOE that governs activities related to national security, non-proliferation, and safety and reliability of nuclear weapons.	http://www.dod.gov/dodgc/olc/docs/2000NDAA.pdf
	DOE	Atomic Energy Act of 1954	Under the AEA, the DOE is authorized to conduct R&D in applications of atomic energy for the U.S. Navy; conduct the Nation's nuclear weapons program; provide for related storage, transportation, and disposal of hazardous and radioactive waste; and regulate the possession, transfer, and use of source, byproduct, and Special Nuclear Material (SNM) to protect public health and safety and to provide for common defense and security.	http://www.nrc.gov/about-nrc/governing-laws.html
	EPA	Energy Policy Act of 2005	Among other activities, Section 651(d) requires establishment of an interagency task force to report to the President and Congress on the security of radiation sources in the U.S. from potential threats, and to develop recommendations for regulatory and legislative changes related to protection and security of sources. Additionally, EPAct requires the Nuclear Regulatory Commission (NRC) to conduct security evaluations, including force-on-force exercises not less than once every 3 years at licensed commercial power reactor facilities.	http://www.epa.gov/oust/fedlaws/publ_109-058.pdf



PS-Prep

Sector-Specific Worksheets

ASIS Worksheet

1. Program Policies and Management

BS25999-2 Worksheet

See NFPA 4.1, BS 3.1, 3.2

3. Planning / 4. Implementation (cont.)

B. Incident Management Response BS 25999-2 4.3 Sector Examples Workspace

See A NFPA 5.1-5, 6.6/6

ASIS 4.4.6

NFPA Worksheet

6. Maintenance, Review and Improvement

NFPA 1600 8 Sector Examples Workspace

See Also:
ASIS SPC.1 4.5/4.6
BS 25999-2 4.4.3/5.1/5.2 6.1/6.2

8.1 Program Improvement	Sector Examples	Workspace
8.1.1 The entity shall improve effectiveness of the program through management review of the policies, performance objectives, evaluation of program implementation, and changes resulting from preventive and corrective action.	NERC PRC - 012 through -017 NERC CIP - 001-1, -008-1, -008-2 NERC EOP - 004-1	
8.1.2* Reviews shall be conducted on a regularly scheduled basis, and when the situation changes to challenge the effectiveness of the existing program.	NERC FAC - 003-1, -501-WECC-1 NERC INT - 001, 003 through 008	
8.1.3 The program shall also be re-evaluated when any of the following occur: (1) Regulatory changes (2) Changes in hazards and potential impacts (3) Resource availability or capability changes (4) Organizational changes (5)* Funding changes (6) Infrastructure, economic, and geopolitical changes (7) Changes in products or services (8) Operational changes	NERC PRC - 002 through 005, 012, 014 through 018 NERC TOP - 007-0 NERC TPL - 001 through 006 NERC VAR - 002, 501 NERC VAR - STD - 002a-1, -002b-1	
8.1.4 Reviews shall be conducted based on post-incident analyses, lessons learned, and operational performance.	DHS TOPOFF California Public Utilities Commission General Order 166, Standards 1-13	
8.1.5 The entity shall maintain records of its reviews and evaluations, in accordance with the records management practices developed under Section 4.8.		

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

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



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

- Managed by FEMA
- Links to Three Standards
- Federal Register Notices
- Press Releases and Fact Sheets

- Critical Infrastructure Learning Series

www.dhs.gov/ciwebinars

- Partnering for Critical Infrastructure Preparedness
- Voluntary Preparedness Standards

- ANAB Web site

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

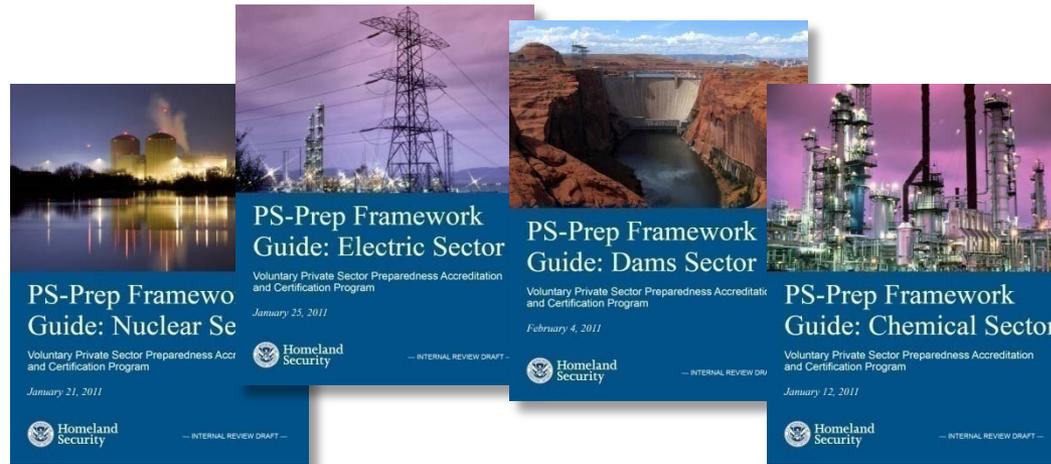
- Cross-reference your chosen preparedness standard with internal programs, policies, best practices and existing regulations that will be relevant to certification
- Gather supporting documentation
- Complete a self-assessment with your internal working team of experts
- Brief the executive sponsor 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



Questions



For more information visit:
www.dhs.gov/criticalinfrastructure

Tracy Shawyer

Director, Partnership and Outreach Division

Tracy.Shawyer@dhs.gov

