Public Law 110-53, Title IX

DATE: Updated 07.20.10

1000 Holcomb Woods Parkway | Suite 130 | Roswell, GA 30076 | 770-643-1114 | **Fax:** 1-800-418-9088

www.firestorm.com

Page Intentionally Left Blank

Public Law 110-53 Title IX
Updated 07.20.10

Update

This white paper has been updated to reflect recent activity within Department of Homeland Security (DHS) regarding its implementation of the PS-Prep program in support of Public Law 110-53. It also has been updated to include Firestorm's assessment of the activity and how the development of PS-Prep should be considered in the implementation of business continuity programs in the private sector.

Executive Summary

Over the past few years, some of the most wide-ranging and demanding financial management and disclosure regulations in U.S. history have been enacted including the Gramm-Leach-Bliley and Sarbanes-Oxley Acts. Failure to comply with these regulations may have serious consequences for you and your company. Currently, the Department of Homeland Security is implementing a certification program for the private sector that promotes preparedness, including **disaster management, emergency management and business continuity programs**. This program, labeled **PS-Prep**, is defined in Public Law 110-53, Section 524.

Business Continuity is a board governance issue. It is a compliance issue. In the past, many businesses have given only lip service to establishing actionable business continuity and disaster recovery plans.

The emergency management focus of this country trends toward response and recovery *during* and *after* a disaster. Rather than perpetuating this disaster denial approach, Firestorm emphasizes readiness *before* disaster strikes. Business Continuity is more than an IT or data recovery issue. Business Continuity is intended to provide assurance that a business can meet their business commitments, no matter what. Business Continuity takes into consideration key employees, critical suppliers, critical vital records, and also the IT equipment, the production environment and data.

Proper disaster planning requires that companies **PREDICT** the vulnerability, **PLAN** the response, and **PERFORM** when the event occurs.

- **PREDICT** Phase: Classifies the critical vulnerabilities, identifies key emergency personnel, ascertains critical decision processes, analyzes gaps, identifies infrastructure and supply chain needs, and defines communications requirements.
- **PLAN** Phase: Develops the strategy, constructs the plan, and involves the appropriate personnel to assure their buy-in and commitment.

- **PERFORM** Phase: Establishes protocols for implementation, community involvement, communications, test exercises, audits, reviews, updates, and compliance. A well designed and executed plan can enable a company in crisis to outperform its competitors and the expectations of its stakeholders. Often, plans are not updated to reflect ongoing changes within organizations, thus creating unforeseen vulnerabilities.

Background

The 9/11 Commission concluded that the United States was not prepared for disasters. America's experiences in Katrina and other natural disasters have reinforced this conclusion, and a renewed sense of urgency exists for creating a national culture of preparedness.

The 9/11 Commission Report stated that:

- ***"Preparedness is a cost of doing business, not a luxury."***
- ***"85% of the U.S. infrastructure is in the private sector."***

The statistics for failure in a disaster are staggering. The United States Department of Labor states that 40% of those companies who are in a disaster never re-open, and 25% of those who do, close within two years. FEMA confirms a 40% to 60% failure for businesses after a disaster. The Red Cross estimates 70,000 disasters occur annually in the U.S. Today, we face the emerging H1N1 (swine flu) pandemic threat, rising fuel costs, terrorism, identity theft, natural disasters, and more.

Senator Joseph Lieberman sponsored legislation to address these concerns. Senator Lieberman felt that private business should play a greater role in preparedness and resilience, and the United States Congress agreed. Congress has enacted Public Law 110-53, entitled "Implementing Recommendations of the 9/11 Commission Act of 2007." Title IX of this Act directs the Department of Homeland Security (DHS) to implement its provisions. DHS is actively implementing these requirements.

Overview of Public Law 110-53, Title IX, PS-Prep

Title IX specifically directs the Department of Homeland Security to "develop guidance or recommendations and identify best practices to assist or foster action in the private sector in:

(1) Identifying potential hazards and assessing risks and impacts;

(2) Mitigating the impact of a wide variety of hazards, including weapons of mass destruction;

(3) Managing necessary emergency preparedness and response resources;

(4) Developing mutual aid agreements;

(5) Developing and maintaining emergency preparedness and response plans, and associated operational procedures;

(6) Developing and conducting training and exercises to support and evaluate emergency preparedness and response plans and operational procedures;

(7) Developing and conducting training programs for security guards to implement emergency preparedness and response plans and operations procedures; and

(8) Developing procedures to respond to requests for information from the media or the public."

There are three separate interrelated components of the PS-Prep Program:

1. **Adoption** – DHS will select one or more appropriate private sector preparedness standards. (This adoption has identified three standards.)
2. **Accreditation** – A DHS-selected entity (ANSI-ASQ National Accreditation Board - ANAB) will establish certification criteria and then manage the process, confirming that third-party qualifications to perform certifications of private sector entities comply with one of the adopted standards. These third parties are "accredited" to provide certifications.
3. **Certification** – An accredited third-party will review and determine that a private sector entity is, in fact, in conformity with one of the preparedness standards adopted by DHS.

As required by the Public Law 110-53, Homeland Security Secretary Janet Napolitano has designated FEMA Administrator Craig Fugate as the officer within DHS to be responsible for overseeing the accreditation and certification program. Mr. Fugate serves as chair of an internal Private Sector Preparedness Coordination Council (PSPCC) comprised of department leadership from the Science & Technology Directorate, Private Sector Office and the Office of Infrastructure Protection.

Activities have been underway in both Adoption and Accreditation. There is, as of this time, no firm date at which point certifications will begin.

DHS's Private Sector Preparedness Council has focused on the remaining requirements of the Act. These include:

- Selecting program standards;
- Defining and promoting the business case for private sector entities to work toward voluntary certification;
- Overseeing the program's progress; and
- Providing regular updates to Congress.

Adoption

Public Law 110-53 (Sections 524) mandates that DHS "shall adopt one or more appropriate voluntary standards that promote preparedness." In December, 2008, DHS posted a notice to the Federal registry calling for recommendations of standards that could possibly be used to drive certifications. Since 2009, DHS has been accepting comments on various standards proposed for consideration.

DHS identified three principles that would be used in determining standards that would be included in the PS-Prep certification program. Those principles include:

1. "To widely encourage private sector preparedness through creation and use of voluntary standards." To encourage the adoption of PS-Prep, DHS is considering numerous standards that are used in the private sector. DHS continues to encourage a standard that will address all the statutory elements of a private sector preparedness standard (disaster management, emergency management and business continuity). Considerations are now including standards that address components of preparedness, as well as any limited standard that might be focused at a specific industry.
2. The PS-Prep program "is to be almost entirely driven by the private sector." DHS has no intent to create new standards, but to leverage those that are already in existence, or might be developed in the future. There is no stated intent to pick a single standard. DHS has also stated that the list of accepted standards will possibly change over time as new versions of existing standards, or new standards, are released.
3. "The designated officer will have discretion to direct the PSPCC's adoption efforts at those private sector standards that meet needs identified by DHS." Stated simply, DHS will not guarantee that any or all proposed private sector standards will be adopted by DHS.

In October 2009, DHS stated their intent, through a posting in the federal Registry, to adopt three standards for use in the PS-Prep certification. Those proposed standards are:

- ASIS SPC.1-2009 "*Organizational Resilience: Security Preparedness, and Continuity Management Systems*"
- British Standard 25999-2:2007 "*Business Continuity Management*"
- National Fire Protection Association 1600:2007 "*Standard on Disaster / Emergency Management and Business Continuity Programs*"

It is anticipated that any private sector entity can select any one of these standards (not a combination of standards) to prepare for and ultimately certify under PS-Prep.

Accreditation

DHS has selected the ANSI-ASQ National Accreditation Board (ANAB) to:

- Develop and oversee the certification process;
- Manage the accreditation; and
- Accredit qualified third parties to carry out the certification in accordance

with the accepted procedures of the program.

ANAB, headquartered in Milwaukee, WI, is an internationally recognized organization that serves the conformity assessment needs of business and industry. ANAB is a certified International Accreditation Forum member and is the only accreditation organization for process/management system certifiers based in the United States.

Once the proposed standards are accepted by DHS, ANAB will be in a position to define the certification process and how third-party organizations will be accredited for their role in certifying individual private sector entities. At present, there is no defined timeframe for the completion of these tasks.

Certification

Certification, in the context of this program, is independent confirmation that a third-party certification organization has validated a private sector entity's emergency preparedness and business continuity management system using one of the accepted standard(s).

The process generally consists of an assessment of the documented program's conformity against the defined standard and an evaluation of the effectiveness of the system's implementation. Once a business is certified, there is a periodic reassessment and audit process so the certifying organization can continue to have confidence in its business's emergency preparedness and business continuity management system's conformity. These certifications will be conducted by certification organizations that are accredited by ANAB for this program.
Private sector organizations, including businesses and critical infrastructure and key resources (CIKR) entities, may apply for certification to the applicable requirements of preparedness standard(s) selected for use in this Program.

Other than brief comments and implied speculation, there are no defined processes as to how organizations will be "certified" under PS-Prep. This process, which must be defined by ANAB, has not yet been made public for input or comments.

Impacts

PS-Prep, combined with other regulations and requirements, creates a burden on business to comply with these identified best practices. Studies have shown the high likelihood of significant loss of shareholder value or bankruptcy in companies due to disasters and crises. Senior leadership will also be judged by the speed and level of resilience of their organizations. Failure to be certified will serve as a theory of liability in lawsuits associated with loss of shareholder value due to natural disasters, terrorism, accidents, and communicable illnesses/pandemics.

Public Law 110-53, Title IX is the next step in a complex pattern of laws and regulations requiring the private sector to develop and maintain business continuity plans.

At this time, there is no civil or criminal fine or penalty for non-compliance under Title IX. However, the law places every business on notice of the need for planning, and outlines key planning requirements, identifies approved standards, creates the need for a third-party certification benchmark, and establishes best practices. The initial DHS strategy is to have the marketplace drive adoption of the certification and will leverage certification as a compliance factor. Title IX discussions indicate that a Sarbanes-Oxley type level of compliance for private sector continuity certification is an ultimate goal.

Many industries are regulated and have previously established continuity and disaster planning requirements. Rating agencies like Standard & Poor's, Moodys', and AM Best include Enterprise Risk Management in their evaluation of corporations. Red Flag Identity Theft and PCI-DSS compliance have specific regulations on information availability with civil and criminal penalties attached thereto.

DHS will publish an annual list of those private sector firms who are certified. Failure of a corporation to be included on the list could impact their ratings, shareholder value, selection as an approved vendor, RFP requirements, government contracts, insurability, and personal liability of senior leadership, D&O coverage, and insurance costs.

Firestorm Analysis

The law is written showing certification of the preparedness of the private sector as voluntary. *"The term 'voluntary preparedness standards' means a common set of criteria for preparedness, disaster management, emergency management, and business continuity programs."*

Although businesses must decide for themselves whether or not to follow the certification process, PS-Prep does require the Department of Homeland Security to "maintain and make public a listing of any private sector entity certified as being in compliance with the program" and provide "guidance or recommendations or best practices as necessary and appropriate." However, for continued listing, an annual or periodic company audit and recertification is required.

Firestorm compliments DHS' focus on preparedness and would encourage an aggressive timetable for continued implementation of PS-Prep. Firestorm actively supports the initiatives being undertaken by DHS and encourages organizations to develop a "culture of preparedness."

The following topics relevant to PS-Prep represent Firestorm's independent thoughts and suggestions for PS-Prep. They are not intended to represent any acceptance from DHS.

- **What about my small business; will we be evaluated and certified under the same process as larger entities?**

  From the initial discussions about PS-Prep, DHS has noted that small businesses should be a special consideration. Certification, particularly a third-party certification, comes with a cost. ANAB will work with DHS to define specifically proposed concepts that might allow organizations classified by the Small Business Association as "small" to be certified in methods that might differ from other private sector entities. This has not yet been determined.

Is there a one-size-fits-all?

Firestorm believes that what is appropriate and reasonable for one organization, due to size or operational environment, might not be sufficient for another. Firestorm supports, and has recommended to DHS, the use of a "maturity model" for certification. Many organizations will have a limited budget that will prohibit the use of paid, third-party agencies to certify their programs. The size of the organization, and its type of business, will be key determinations that should be included in a maturity model. A tiered structure would allow organizations to demonstrate their current state and their maturity/advancement.

Firestorm supports the incorporation of a maturity model and varying options of certification. For instance, there could be three tiers of certification: Gold, Silver, and Bronze. Bronze could represent a self-certification through a standard self-assessment model. Silver could represent a peer-to-peer review and certification, following preset guidelines. Gold could represent a certification from a third-party accredited firm that would complete a comprehensive internal review and issue a Gold certification.

It's a voluntary program – why bother?

To change Public Law 110.53, Title IX to make the PS-Prep program mandatory, or to include incentives or penalties, would require legislative action. This cannot be done by DHS. So, it seems a fair assumption that the law will remain a voluntary certification program. However, DHS has also stated that it projects that the private sector will drive itself into the PS-Prep certification through competition and supply chain demand.

Today, it is a best practice that organizations understand the risk they have, relevant to key vendors and their supply chain. "Failure of a Critical Supply Chain" is one of the five common failures Firestorm finds when reviewing business continuity programs. The PS-Prep certification would be an automatic stamp of preparedness.

As a voluntary program, Firestorm anticipates the supply chain will drive participation in a reasonable program. Firestorm encourages private sector entities to use the PS-Prep certification as a means of measuring the preparedness of key suppliers/vendors. Also, anticipate that key customers will begin to ask private sector entities about their own programs – Are you PS-Prep certified? You may find your company can leverage PS-Prep certification as a competitive advantage.

Should I do anything now, or just wait?

While the PS-Prep certification process has not been formally announced, waiting will put extreme pressure on organizations once the certification process is announced. With the proposed standard now announced, organizations should begin to prepare now by making adjustments to their programs. With limited budgets and limited resources, taking advantage of the window of preparation will be a tremendous return on the investment once the certification process is formally announced.

How do I prepare?

The discipline of Firestorm's **PREDICT**. **PLAN. PERFORM.** model works well to build a roadmap for PS-Prep readiness.

PREDICT.

The first step in preparing is to understand your organization's level of preparedness. You know what you know; you do not know what you don't know.

Organizations will need to know where their current business continuity program aligns, at a high level, to the standards that are being announced. Firestorm's Business Continuity Self-Assessment is designed to provide a HIGH LEVEL assessment of an organization's "Preparedness" and is intended as a diagnostic tool to prioritize decisions from a return on investment perspective.

The Self-Assessment is a series of 50+ questions that are divided across the following areas of a Business Continuity Program:

- Program Policy
- Risk Assessment
- Business Impact Analysis
- Strategy
- Plans
- Maintenance
- Testing and Exercises
- Training and Awareness
- Crisis Communications
- Incident Response
- Communicable Illness

Through a one-on-one interview with key contacts for business continuity, Firestorm engages in a conversational series of questions that allow you to "self-assess" against 50+ key points. Each question is designed to capture a specific, structured response from multiple-choice selections. Upon completion of all questions, the Self-Assessment produces a chart demonstrating overall scoring percentages by the above key areas, as well as an overall ranking of program "readiness" and a narrative analysis.

Following the one-on-one interview, Firestorm analyzes the results and follows up with a report and discussion of the rating.

Plan.

With the Firestorm's self-assessment and analysis completed, you can begin to define a roadmap for activities over the next 18-24 months that will prepare your organization for certification once the process is announced.

Perform.

Whether or not you elect to acquire PS-Prep certification is a decision that can be delayed until additional information is available. However, the self-assessment completed in the Predict phase will allow you today to begin implementing incremental improvements/adjustments to your business continuity program that will bring value to your organization's overall preparedness.

Firestorm offers the following thoughts beyond the questions that were included in the Registry:

Monitoring/Triggers – The proposed standards incorporate the best practices as defined in the industry, but leave one area without definitive guidelines. As Firestorm has worked with customers, one of the five common failures is a failure to identify and monitor all vulnerabilities. While a vulnerability/risk assessment is part of each standard, each standard falls short in requiring that triggers be developed, with defined monitoring guidelines. In Firestorm's experience, without defining triggers and the monitoring for those triggers, there is an unfortunate tendency to miss an appropriate "call to action."

Need for an Educational Portal – For PS-Prep to be generally accepted, many organizations will need to educate employees to be proficient in the concepts of preparedness. Information is constantly changing and the techniques that have been used in the past (traditional classroom offerings) are too expensive, and limited by travel restrictions and budget. A portal offering educational content to develop and enhance business continuity skills, with on-demand training and information will be key to preparing individuals to develop programs for their organization. Firestorm encourages DHS to promote and sponsor the development of such a concept and Firestorm is willing to contribute content to such a portal.

First Response for Business – While FEMA focuses on recovery for individuals and the public sector, FEMA leaves a gap for businesses during any emergency. There needs to be a simple, low-cost solution where businesses can gain access to support services and supplies inventory on a priority basis.

About Firestorm

Firestorm is a national leader in crisis communications & management, emergency response and business continuity consulting services. Firestorm's mission is to build strong *Disaster Ready People* and *Disaster Ready Businesses*. Firestorm focuses on establishing nationwide private sector readiness before disaster strikes.

Firestorm specializes in disaster mitigation by helping organizations identify vulnerabilities and establish appropriate enterprise programs for business continuity and crisis management. Firestorm's services help clients protect their employees, assets, revenues, reputation and, ultimately, the value to all stakeholders. Firestorm services are designed to include emphasis on the human component in every crisis. Firestorm's core philosophy is '*Every Crisis is a Human Crisis'*, and this philosophy is embedded into all recommendations and implementations, to ensure organizations focus on people, processes, and procedures.

Firestorm differentiates itself from other business continuity service providers with its unique PREDICT. PLAN. PERFORM.™ process. Firestorm deliverables include critical decision support and crisis management, communicable illness/pandemic plans, emergency operations and disaster recovery plans, vulnerability analyses and risk assessments, as well employee/client training and presentations.

Firestorm serves its network of clients through offices in Atlanta, Denver and New York, and is staffed by attorneys, engineers, and business continuity professionals. In addition, Firestorm utilizes its Expert Council™ which is comprised of recognized specialists from various disciplines, professions and industries. Together with the Firestorm Solutions Board™, these talented individuals bring a level of credibility and skill to the planning process which cannot be matched by any other organization. It is the breadth and depth of Firestorm's human capital that distinguishes Firestorm from other consulting firms.

For more information, please contact us at 1-800-321-2219 or visit our website at www.firestorm.com.