The State Office of Risk Management

The State Office of Risk Management was created in 1997 by the 75th Texas Legislature through House Bill 2133, merging the responsibilities of the Risk Management Division of the Texas Workers' Compensation Commission under Chapter 412, Texas Labor Code, with the duties of the Workers' Compensation Division of the Attorney General's Office under Chapter 501, Texas Labor Code. SORM's responsibilities have been expanded by the Texas Legislature over time, including in 2001, when the 77th Texas Legislature passed House Bill 1203, expanding SORM's mission to include serving as a full service risk and insurance service manager to reduce property and liability losses, later expanded to include oversight of continuity of operations for the state.

Today, I serve as the State Risk Manager for Texas, overseeing the State Office of Risk Management as Executive Director. The Office administers the enterprise risk and insurance management programs, continuity of government operations program, and self-insured workers' compensation program for the State of Texas.

Source: Texas Legislature Online, "An Act," accessed September 1, 2016, http://www.capitol.state.tx.us/tlodocs/75R/billtext/html/HB02133F.htm

Basic Planning and Preparation

In the event of a catastrophe or disaster, consequences of an incident may interrupt essential operations of government entities. The practical effect of these events is an adverse impact on the clients of government entities, whether these are other governmental units or the general public. To prepare for such interruptions, government entities have various available protocols for plans to respond to those events and resume essential functions, each with a potentially different emphasis and level of detail and complexity.

Examples of available plans in use include, but are not limited to, business continuity plans, continuity of operations plans, continuity of government plans, crisis communications plans, critical infrastructure protection plans, cyber incident response plans, disaster recovery plans, information system contingency plans, emergency operations plans, occupant emergency plans, and others.

Source: Stephen Vollbrecht, BLUEPRINTS FOR DISASTER: BALANCING SECRECY AND TRANSPARENCY OF GOVERNMENT CONTINUITY PLANS, Note 6, https://www.hsdl.org/?view&did=796508

The difference between the two highlighted plans is outlined below.

What is a Continuity of Operations Plan (COOP)?

Continuity of Operations (COOP), as defined in the National Continuity Policy Implementation Plan (NCPIP) and the National Security Presidential Directive-51/Homeland Security Presidential Directive-20 (NSPD-51/HSPD-20), is an effort within individual executive departments and agencies to ensure that Primary Mission Essential Functions (PMEFs) continue to be performed during a wide range of emergencies, including localized acts of nature, accidents and technological or attack-related emergencies.

This is the standard adopted by SORM as the Texas framework.

Source: https://www.fema.gov/pdf/about/org/ncp/coop_brochure.pdf

What is an IT Disaster Recovery Plan (DR)?

Businesses use information technology to quickly and effectively process information. Employees use electronic mail and Voice Over Internet Protocol (VOIP) telephone systems to communicate. Electronic data interchange (EDI) is used to transmit data including orders and payments from one company to another. Servers process information and store large amounts of data. Desktop computers, laptops and wireless devices are used by employees to create, process, manage and communicate information. What do you when your information technology stops working?

An information technology disaster recovery plan (IT DRP) should be developed in conjunction with the business continuity plan. Priorities and recovery time objectives for information technology should be developed during the business impact analysis. Technology recovery strategies should be developed to restore hardware, applications and data in time to meet the needs of the business recovery.

Businesses large and small create and manage large volumes of electronic information or data. Much of that data is important. Some data is vital to the survival and continued operation of the business. The impact of data loss or corruption from hardware failure, human error, hacking or malware could be significant. A plan for data backup and restoration of electronic information is essential.

SORM has not specifically authorized to designate a statewide standard/framework for IT planning.

Source: https://www.ready.gov/business/implementation/IT

The following are the relevant statutory provisions of potential interest to the Committee:

Texas Labor Code 412.054:

Sec. 412.054. CONTINUITY OF OPERATIONS PLAN. (a) Each state agency shall work with the office to develop an agency-level continuity of operations plan that outlines procedures to keep the agency operational in case of disruptions to production, finance, administration, or other essential operations. The plan must include detailed information regarding resumption of essential services after a catastrophe, including:

(1) coordination with public authorities;

(2) management of media;

(3) customer service delivery;

(4) assessing immediate financial and operational needs; and

(5) other services as determined by the office.

(b) A continuity of operations plan that meets the requirements of this section must be submitted by each state agency that is:

(1) involved in the delivery of emergency services as a member of the governor's Emergency Management Council;

(2) part of the State Data Center program; or

(3) subject to this chapter or Chapter 501.

(c) Except as otherwise provided by this section, the following information is confidential and is exempt from disclosure under Chapter 552, Government Code:

(1) a continuity of operations plan developed under this section; and

(2) any records written, produced, collected, assembled, or maintained as part of the development or review of a continuity of operations plan under this section.

(d) Forms, standards, and other instructional, informational, or planning materials adopted by the office to provide guidance or assistance to a state agency in developing a continuity of operations plan under this section are public information subject to disclosure under Chapter 552, Government Code.

(e) A state agency may disclose or make available information that is confidential under this section to another state agency, a governmental body, or a federal agency.

(f) Disclosing information to another state agency, a governmental body, or a federal agency under this section does not waive or affect the confidentiality of that information.

Added by Acts 2007, 80th Leg., R.S., Ch. 407 (S.B. 908), Sec. 11, eff. September 1, 2007.
Amended by:

Acts 2015, 84th Leg., R.S., Ch. 1045 (H.B. 1832), Sec. 4, eff. June 19, 2015.

Texas Government Code 2054.518:

Sec. 2054.518. CYBERSECURITY RISKS AND INCIDENTS. (a) The department shall develop a plan to address cybersecurity risks and incidents in this state. The department may enter into an agreement with a national organization, including the National Cybersecurity Preparedness Consortium, to support the department's efforts in implementing the components of the plan for which the department lacks resources to address internally. The agreement may include provisions for:

(1) providing fee reimbursement for appropriate industry-recognized certification examinations for and training to state agencies preparing for and responding to cybersecurity risks and incidents;

(2) developing and maintaining a cybersecurity risks and incidents curriculum using existing programs and models for training state agencies;

(3) delivering to state agency personnel with access to state agency networks routine training related to appropriately protecting and maintaining information technology systems and devices, implementing cybersecurity best practices, and mitigating cybersecurity risks and vulnerabilities;

(4) providing technical assistance services to support preparedness for and response to cybersecurity risks and incidents;

(5) conducting cybersecurity training and simulation exercises for state agencies to encourage coordination in defending against and responding to cybersecurity risks and incidents;

(6) assisting state agencies in developing cybersecurity information-sharing programs to disseminate information related to cybersecurity risks and incidents; and

(7) incorporating cybersecurity risk and incident prevention and response methods into existing state emergency plans, including continuity of operation plans and incident response plans.

(b) In implementing the provisions of the agreement prescribed by Subsection (a), the department shall seek to prevent unnecessary duplication of existing programs or efforts of the department or another state agency.

(c) In selecting an organization under Subsection (a), the department shall consider the organization's previous experience in conducting cybersecurity training and exercises for state agencies and political subdivisions.

(d) The department shall consult with institutions of higher education in this state when appropriate based on an institution's expertise in addressing specific cybersecurity risks and incidents.

Added by Acts 2017, 85th Leg., R.S., Ch. 683 (H.B. 8), Sec. 11, eff. September 1, 2017.