Hardening of Utility Facilities and Critical Infrastructure

HB 2320

State of Texas

November 2020

Table of Contents

Executive Summary

On a daily basis, citizens throughout Texas rely on public and private entities to supply basic services such as water, wastewater, electricity, internet, telephone service, transportation, hospitals, and public safety through critical infrastructure. These systems have a significant beneficial impact on the lives of Texans, including to their health, safety, economic interests, and social interactions. In the event of a man-made or natural disaster, the viability of these systems can also mean the difference between life and death. If a disaster causes the degradation of service in one of these areas, it can have both immediate and long-term impacts on the community, region, state, and nation.

To ensure that all practical efforts are made to ensure the continuity of operations of critical infrastructure, public and private entities as well as private citizens need to take steps to protect these vital components. While each individual facility will require different solutions to protect against interruption of service, this plan provides a methodology to build resilience across these sectors. The following actions through the associated recommendations will provide the foundation for resilience and include 1) identifying critical infrastructure statewide, 2) encouraging risk assessments be conducted at critical infrastructure facilities, 3) developing a site-specific plan to mitigate against threats, risks and hazards, 4) integrating critical infrastructure owners and operators in the development and implementation of state and local emergency operations and hazard mitigation plans, 5) developing support to fund resilience efforts critical infrastructure, 6) provide information on potential threats and hazards to critical infrastructure owners and operators, 7) protect information regarding critical infrastructure, 8) Request an update to the Infrastructure Protection Report Series, and 9) encourage a risk assessment for proposed critical infrastructure facilities.

The capacity of local, state, and federal entities as well as the private sector to mitigate potential impacts to critical infrastructure improves the ability of communities to prepare for, respond to, and recover from disasters and Texans to continue their day-to-day lives supporting their families and communities.

Overview

Purpose

This document addresses the legislative mandate from House Bill 2320 from the 86th Regular Legislative Session by identifying methods to harden and reduce risks and impacts on utility facilities, critical infrastructure, hospitals and fire departments from a disaster, and encouraging public and private entities that are responsible for these facilities to implement the plans required to reduce the exposed risks.

The recommendations offered within this document are designed to supply critical infrastructure owners and operators with guidance to identify and utilize the available federal, state, local and private resources and tools shown to be beneficial in maintaining continuous operations of essential services throughout a disaster. The document also provides recommendations regarding steps that can be taken at the local, state and federal governmental levels to provide support for these facilities. This document will provide recommendations to address the common disaster mitigation operational best-practices but does not address site-specific mitigation strategies.

Critical infrastructure includes all public or private assets, systems, and functions vital to the security, governance, public health and safety, economy, or morale of the state or the nation.

Goal

The goal of this report is to provide a clear process for owners and operators of critical infrastructure to plan for and mitigate against damage caused by disasters which could interrupt operations and to encourage them to participate in these actions.

Objectives

To increase the resilience of critical infrastructure and improve the ability to maintain operations during and after a disaster, the following objectives must be addressed:

- Develop and continually update a comprehensive statewide inventory and contact list of critical infrastructure facilities and systems;
- Encourage the development of risk assessments of each facility on the critical infrastructure inventory;
- Develop, implement, exercise and regularly update a critical infrastructure protection plan (CIPP);
- Ensure Community Lifelines owners and operators are included in the development of the jurisdiction's hazard mitigation and disaster recovery planning;
- Build support for funding of the critical infrastructure protection plans by gathering and sharing data as well as educating the general public and key stakeholder groups;
- Provide timely information to critical infrastructure owners and operators of potential threats and disasters which may impact their facilities;
- Protect the information regarding critical infrastructure to ensure that these facilities are not targeted for disruption;
- Request the Cybersecurity and Infrastructure Security Agency to update the Infrastructure Protection Report Series; and
- Encourage proposed Critical Infrastructure Projects to conduct a Risk Assessment of a potential facility location and design prior to construction.

Audience

- Critical Infrastructure Stakeholders
- Local Jurisdictions
- Texas State Legislature
- Texas State Agencies
- Federal Agencies

Authority

House Bill 2320

Authors:	Representative Dennis Paul (District 129)
Co-Authors:	Multiple co-authors
Sponsor:	Senator Larry Taylor - District 11
Co-sponsor:	Senator Eddie Lucio, Jr. - District 27

For more information: Texas Legislature Online to Section 418.055

https://capitol.texas.gov/tlodocs/86R/billtext/pdf/HB02320F.pdf#navpanes=0.

Stakeholders

Agent	Summary
Texas Division of Emergency Management (TDEM)	The Texas Division of Emergency Management is charged with carrying out a comprehensive all-hazard emergency management program for the state and for assisting cities, counties, and state agencies in planning and implementing their emergency management programs.
Texas Railroad Commission	The Commission oversees the development of the state's energy resources, advances safety in the delivery and use of Texas petroleum products, and protects the environment and consumers by ensuring that energy production, storage, and delivery prevent or minimize harmful effects on the state's natural resources.
Texas Commission on Environmental Quality (TCEQ)	The Texas Commission on Environmental Quality strives to protect our state's public health and natural resources consistent with sustainable economic development. To accomplish our mission, we will: • base decisions on the law, common sense, sound science, and fiscal responsibility; • ensure that regulations are necessary, effective, and current; • apply regulations clearly and consistently; • ensure consistent, just, and timely enforcement when environmental laws are violated; • ensure meaningful public participation in the decision-making process; • promote and foster voluntary compliance with environmental laws and provide flexibility in achieving environmental goals; and • hire, develop, and retain a high-quality, diverse workforce.
Texas Engineering Extension Service (TEEX)	It comes down to saving lives. From providing emergency responders to disasters across the state and nation to developing training and practical workforce solutions, TEEX makes a difference worldwide. More than 200,000 people representing every U.S. state and territory and 105 countries are served annually through on-site and online resources for specialties from homeland security to economic development and workforce training. Texas A&M Task Force 1 and Texas Task Force 2, the state's elite urban search and rescue teams, are sponsored by TEEX.
Texas Department of Public Safety (DPS). Office of Critical Infrastructure Protection (OCIP)	The Texas Department of Public Safety Office of Critical Infrastructure Protection is a component of the Texas Office of Homeland Security and works closely with the Intelligence and Counterterrorism Division—thus leveraging capabilities in both criminal intelligence and emergency preparedness and response. OCIP coordinates with Texas critical infrastructure partners in each of the 16 identified sectors, in order to: maintain situational awareness of threats and hazards; share threat information and guidance; collect, manage, and analyze state-level infrastructure data; support the Texas

	State Operations Center and infrastructure stakeholders during disasters; and help facilitate critical infrastructure protection efforts across the state. Additionally, OCIP administers the Texas Infrastructure Liaison Officer Program.
Public Utility Commission of Texas (PUC)	The Public Utility Commission of Texas exists to serve Texans by regulating the state's electric, telecommunication, and water and sewer utilities, implementing respective legislation, offering assistance in resolving consumer complaints and overseeing disaster preparation and recovery efforts by utilities. Since its founding in 1975, the Commission has a long and proud history of service to Texas, protecting customers, fostering competition, and promoting high quality infrastructure.
Texas Department of Transportation (TxDOT)	The Texas Department of Transportation (TxDOT) mission is: Through collaboration and leadership, we deliver a safe, reliable, and integrated transportation system that enables the movement of people and goods. The TXDOT Vision is to be a forward-thinking leader delivering mobility, enabling economic opportunity, and enhancing quality of life for all Texans.
Cybersecurity and Infrastructure Security Agency	The Cybersecurity and Infrastructure Security Agency (CISA) is the Nation's risk advisor, working with partners to defend against today's threats and collaborating to build more secure and resilient infrastructure for the future.
The Honorable Nate McDonald	Matagorda County Judge
Aoife Longmore	Austin Department of Homeland Security and Emergency Management – Program Manager
Miranda Hahs	Montgomery County Office of Homeland Security and Emergency Management – Senior Planner
Chris Hogan	Port of Freeport – Director of Protective Services
Carey Morgan	Hays County Office of Emergency Management
Darrian Hudman	City of Corrigan – City Manager
Robert Harrell	Coryell County Office of Emergency Management – Emergency Management Coordinator
Mark Morgan	City of Galveston – Emergency Management Coordinator
Bill Vola	Chambers County – Deputy Emergency Management Coordinator
Jeremiah Lancaster	City of Plano – Chief Technology Officer
Stacy Moore-Guajardo	Lower Colorado River Authority – Emergency Management Program Manager

Background, Discussion & Recommendations

The state of Texas has received more federal disaster declarations than any other state in addition to the numerous state disasters that failed to meet federal thresholds and requirements. Although predicting every future disaster ahead of time is not likely, the state can learn from past disasters and prepare for future disasters through the adoption of laws, policies and procedures designed to diminish the impact of similar disasters.

Critical infrastructure is a term which may vary from one entity to another. For the purposes of this document, "critical infrastructure" will be deemed to include all public or private assets, systems and functions vital to the security, governance, public health and safety, economy, or morale of the state. Although House Bill 2320 specifically excluded "a utility facility owned or controlled by a utility regulated by the Public Utility Commission of Texas," and specifically includes hospitals and fire stations, the recommendations contained in this report may be applied across any components of critical infrastructure.

Owners and operators of critical infrastructure facilities that have the potential to substantially impact a community's sustainability before, during and after a disaster are ultimately responsible for identifying, reducing or minimizing risks, and exercising their continuity of operations plans. The failure to implement these plans by one key infrastructure sector can have cascading consequences to any community including the impact on other interrelated sectors. As a result, federal, state, and local jurisdictions also have a vested interest in the sustainability of critical infrastructure within their boundaries and should be engaged to ensure the facilities are constructed, maintained and fortified in a manner capable of minimizing a disruption to operations.

Laws, policies, rules, and procedures all have a hand in governing infrastructure sectors. In some scenarios, the ability for critical infrastructure facilities to minimize risks may be delayed or prohibited due to government restrictions, limited funding, or lack of planning. Although critical infrastructure facility owners and operators are ultimately responsible for reducing or minimizing risks that have the potential to substantially impact the normal operations of systems considered to be critical infrastructure during a disaster, the solution requires a concerted effort between the public and private sectors.

Reducing or minimizing the risks that would substantially impact a business' or organization's ability to sustain normal operations during a disaster should be a goal for all business and industry leaders. Owning or operating a business or facility that has been deemed critical infrastructure elevates this notion to a primary goal.

As the state prepares for disasters and their impact on critical infrastructure it is important to identify the vast array of disaster types with examples of each. Communities, and the critical infrastructure within them, may experience various hazards or threats as the result of natural, technological or human-caused disasters, which all have the potential to harm, damage, incapacitate or destroy critical infrastructure. The examples below are intended to identify most potential hazards and threats of concern to critical infrastructure

Hazard Type	Definition	Examples
Natural	Result from acts of nature	Drought, Earthquake, Epidemic, Flood, Hurricane, Landslide, Tornado, Subsidence/Sinkhole, Hail, Tsunami, Volcanic Eruption, Wildfire, Winter Storm, and Severe Wind
Technological	Result from accidents or the failures of systems and structures	Airplane Crash, Dam/Levee Failure, Hazardous Materials Release, Power Failure, Radiological Release, Electromagnetic Pulse, Train Derailment, and Urban Conflagration

Human-Caused	Result from the intentional actions of an individual or organized group of individuals	Civil Disturbance, Cyber Incidents, Sabotage, School Violence, and Terrorist Acts

Just as important as planning for likely disasters is identifying critical infrastructure.

Critical Infrastructure Sectors

- Chemical
- Commercial Facilities
- Communications
- Critical Manufacturing
- Dams
- Defense Industrial Base
- Emergency Services
- Energy
- Financial Services
- Food and Agriculture
- Government Facilities
- Healthcare and Public Health
- Information Technology
- Nuclear Reactors, Materials, and Waste
- Transportation Systems
- Water and Wastewater Systems

Where each sector is vital to the state for apparent reasons, there are seven Community Lifelines, which were formalized in 4th Edition of the National Response Framework, recognized as being so critical that a disruption or shut down by one of these functions will directly affect the security and resilience of critical infrastructure within and across numerous sectors. The designated community lifelines during most disasters are – safety and security; food, water, and shelter; health and medical; energy; communications; transportation; and hazardous material.

Currently, the Cybersecurity and Infrastructure Security Agency has compiled information on specific types of critical infrastructure facilities. This information includes the Infrastructure Protection Report Series which outlines the risks and threats that facilities from critical infrastructure sectors may face, and recommendations to reduce the potential for them to negatively impact the facilities. Sector owners and operators may currently obtain these reports through the Cybersecurity and Infrastructure Security Agency.

The Texas Department of Public Safety, Office of Homeland Security, Office of Critical Infrastructure Protection also develops plans and information to be used by critical infrastructure sectors in Texas which highlight descriptions of and potential threats to these sectors. OCIP most recently updated and published *Texas: Critical Infrastructure Profile* report in October of 2019.

Recommendations

OBJECTIVE 1. Develop and continually update a comprehensive statewide inventory and contact list of critical infrastructure facilities and systems.

Discussion

There are thousands of critical infrastructure facilities throughout Texas, the identification of, and communication with, critical infrastructure owners and operators is a key component of increasing the resilience of these facilities that are vital to the economic, social and physical health of Texas. To improve the ability of these facilities to be protected against disasters Texas must be able to communicate directly with each individual facility, or the owner/operator, in a timely manner and to be

able to incorporate these facilities into the mitigation planning at the local and state levels. This effort will require collaboration between the Texas Department of Public Safety, Texas Office of Homeland Security, the Texas Division of Emergency Management, the Public Utility Commission, the Texas Commission on Environmental Quality, the Cybersecurity and Infrastructure Security Agency, the Texas Railroad Commission, local jurisdictions and individual owners and operators.

Currently there are several state and federal agencies which collect information on these facilities for the purposes of regulation, mitigation, and protection. To effectively assist with the development of a statewide inventory, the consolidation of this information and the coordination of communications regarding potential impacts must occur. For instance, DPS maintains the TxMAP system which houses 390 unique data sets covering thousands of facilities and all 16 critical infrastructure sectors. This resource is restricted access to ensure that the locations and vulnerabilities of the facilities may not be used to target those facilities, but also limits its utility in collaborative planning efforts at the local and state levels. The information does not include specific contact information for each facility or owner/operator.

Recommendation 1: Develop and Validate a statewide inventory and contact list for critical infrastructure facilities, beginning with the Community Lifelines.

The Texas Division of Emergency Management should collaborate with local, state and federal partners to develop a single point of contact with critical infrastructure owners and operators for the purpose of creating a comprehensive map and listing of these facilities. The development of this resource will necessitate the cooperation of state and federal agencies to prepare the initial listing of facilities. The development of the statewide inventory should begin with the Community Lifelines within each TDEM disaster district to ensure that those that are of most crucial importance to the state and locality are incorporated as quickly as possible. As these sectors are developed in the inventory, additional sectors can be added as determined by the state and its local and federal partners.

Recommendation 2: Share critical infrastructure list and contacts with local jurisdictions.

Once developed, sections of the Critical Infrastructure List, specific to the locality, should be shared with local jurisdictions to ensure that local hazard mitigation planning includes these facilities in the development, exercise and implementation of plans to improve protection and resilience of these jurisdictions. The information on the location and points of contact for these facilities should be handled in a secure fashion with protections to ensure that such data is only available to designated state and local jurisdiction-designated contacts and is not subject to open records requests or public dissemination.

Objective 2: Encourage the development of risk assessments of each facility on the critical infrastructure inventory.

Discussion

Risk and vulnerability assessments are critical to the development of plans to protect facilities and build resilience against interruption of critical services. Although individual facilities will need to conduct these assessments at the site level, there are national, state and local resources which may be used in the development of these assessments. Many of these facilities will already have in place assessments and mitigation plans for their own purposes or to meet existing regulation. Duplication of effort is not beneficial to the goal of increasing resilience, and existing plans should be used where viable.

At the federal level the National Infrastructure Protection Plan (NIPP) provides a framework to "[s]trengthen the security and resilience of the Nation's critical infrastructure, by managing physical and cyber risks through the collaborative and integrated efforts of the critical infrastructure community." This plan provides a broad description of the steps necessary to develop and implement plans across all critical infrastructure facilities in the country.

The National Risk and Capability Assessment provides standardized methods to determine the risk and capability of the nation to respond to challenges brought about by threats and hazards. The Threat and Hazard Identification and Risk Assessment (THIRA) provides a three-step risk assessment process to help communities understand their risks and how to address them proactively. The National THIRA provides a review of the most challenging types of threats and hazards that can impact the nation as a whole and the capability that would be needed to respond to these events. These assessments can be used at individual facilities to provide information on applicable threats.

The Cybersecurity and Infrastructure Security Agency previously developed the Infrastructure Protection Report Series which outlines the risks and threats that critical infrastructure sectors may face, and recommendations to reduce the potential for them to negatively impact the facilities. Although these reports have not been updated since 2013 and are no longer being produced by CISA, the use of these reports by individual sector owners and operators may still provide valuable information on the threats posed and the steps to reduce these threats.

The state of Texas also provides significant information on the risks and hazards which may affect critical infrastructure. The State Hazard Mitigation Plan (SHMP) must contain analyses of relevant natural hazards, and identification of strategies and actions to address them. These examinations of underlying hazard exposure include geography, population and the built environments, identification and analysis of the nature of the hazards, analysis of historical impacts, and assessment of future risks related to the identified hazards. The Texas Geographic Society (TXGS) has worked with TDEM to support the hazard identification and risk assessment planning since 2002. In 2013, TXGS published the first Community Hazard Analysis and Mitigation Planning Support Reports (CHAMPS '13). These were released in 254 volumes: one for each county in Texas. The objective of these reports was to provide hazard analysis information that local communities could use in developing their hazard mitigation plans.

TDEM and the State Hazard Mitigation Team decided that CHAMPS '17 would focus at the state level and take a more comprehensive approach than was taken in the CHAMPS '13 Reports. Specifically, CHAMPS '17 would not only analyze historical patterns of natural hazards but also assess future risks. For this reason, CHAMPS '17 has been developed as a statewide hazard assessment. In the early summer of 2018, TXGS released CHAMPS '18. The reports are intended to extend the benefits of this new, more inclusive approach to counties. CHAMPS '18 also includes information on the mitigation priorities established by the state through this revision of its mitigation plan. TXGS's objective is to promote common understanding of natural hazards and aligned strategies to deal with those hazards.

The Cybersecurity and Infrastructure Security Agency (CISA), Infrastructure Security Division provides Protective Security Advisors (PSAs), who are subject matter experts in critical infrastructure protection and vulnerability mitigation, to local, state and private sector entities. Through this program, the PSAs focus on supporting five mission areas:

1) Planning, coordinating, and conducting security and resilience surveys and assessments;
2) Planning and conducting outreach activities and providing access to critical infrastructure security and resilience resources, training and information;

3) Supporting National Special Security Events like the Super Bowl,
4) Serving as Liaisons between federal and local government officials and private sector critical infrastructure owners and operators during and after an incident; and
5) Coordinating and supporting improvised explosive device awareness and risk mitigation training, as well as CISA's Cybersecurity Division assessments and resources.

Facility owners and operators with the assistance of the Protective Security Advisors may utilize the Infrastructure Survey Tool (IST) which is a voluntary, web-based security survey to identify and document the overall security and resilience of the facility. The security survey is conducted to:

- Identify facilities' physical security, security forces and management, information sharing, protective measures, and dependencies related to preparedness, mitigation, response, resilience and recovery.
- Identify security gaps.
- Create facility protective and resilience measure indices that can be compared to similar facilities.
- Track progress toward improving critical infrastructure security.

Recommendation 3: Encourage development of site-specific risk assessments of Critical Infrastructure beginning with Community Lifelines.

Based upon the information for the locality in which the critical infrastructure is located, critical infrastructure owners and operations should be encouraged to conduct a site-specific risk assessment to review the potential for threats and hazards to a specific site. These can be identified through coordination with CISA, DHS Office of Intelligence and Analysis, the Texas Department of Public Safety Fusion Centers, local law enforcement and state and local hazard mitigation planners. The purpose of a site-specific risk assessment is to identify threats and hazards, determine effective actions for mitigation, increase public safety, and reduce the threat of future property damage or loss of life. These plans should consider existing state and/or local hazard maps; prior evidence of hazard history; and on-site features such as topography, soils, forests, water channels, and other structures to determine risk level of or to the proposed development.

Objective 3: Develop, implement, exercise and regularly update a critical infrastructure protection plan (CIPP).

Recommendation 4: Encourage Community Lifelines owners and operators to develop site-specific Critical Infrastructure Protection Plans.

Once an assessment of the potential threats and hazards that could affect critical infrastructure has been conducted, owners and operators of these facilities should act by regularly exercising and evaluating evolving hazards and appropriately planning to mitigate the risks. These entities should review applicable local and state hazard mitigation plans and partner with jurisdictions on projects that impact their facilities and operations. A key aspect of these efforts is the development of a Critical Infrastructure Protection Plan (CIPP).

A Critical Infrastructure Protection Plan (CIPP) is a written strategy to make critical infrastructure more resilient. As the National Academy of Sciences defined in Disaster Resilience: A National Imperative, *"…resilience is the ability to prepare and plan for, absorb, recover from and more successfully adapt to adverse events."* Critical Infrastructure owners and operators in conjunction with their stake holders should develop and exercise a plan that improves resilience. Failure to take these actions to

acknowledge and mitigate the hazards identified in the assessments may lead to failure of the infrastructure thereby adding a secondary disaster to an already impacted community.

The National Infrastructure Protection Plan, the Texas State Hazard Mitigation Plan and local hazard mitigation plans provide detailed information related to natural hazards, and certain technological risks. There are numerous ways for a critical infrastructure owner or operator to minimize the risks to these facilities. Currently, these facilities may be required to develop Emergency Operations Plans, Continuity of Operations Plans, and Physical and Cyber Security plans. Each of these types of plans provides support to reduce the vulnerability of these facilities to damage or loss of operational capacity. The CIPP should incorporate these components as well as the mitigation strategies.

To better focus limited resilience funding, owners and operators should prioritize resilience funding toward those projects which will be most effective to limit the impact of the highest risk events. This prioritization should evaluate the potential consequences to the facility for failing to mitigate against those risks, hazards and threats; the likelihood of the threat; the severity of the damage that could result if the threat occurs; and the availability of funding to mitigate against these threats. Each facility must evaluate these factors when prioritizing the availability of funding and should include such prioritization in their CIPP.

The development of the CIPP must be reviewed and updated on an ongoing basis as the facility changes, is updated, or declines in importance. Maintaining an up to date CIPP and risk assessments is critical to ensuring that efforts made to mitigate are relevant and will provide meaningful protection to the facility. Due to the extensive number and type of facilities at risk, the variable nature of threats against those facilities, and the viability of various solutions, the information in Appendix 1 can be used as a starting point in the development of a CIPP, but the practical application of these efforts will require expert assistance that can provide site specific recommendations.

Objective 4: Ensure Community Lifelines owners and operators are included in the development of the jurisdiction's hazard mitigation and disaster recovery planning.

Recommendation 5: State and Local Hazard Mitigation planning processes should include Community Lifeline owners and operators for facilities within the jurisdiction.

The development of local hazard mitigation plans should include Community Lifeline owners and operators regardless of public or private ownership. This will help to ensure that the prioritization of any funds received by local jurisdictions to mitigate against disasters includes consideration of all potentially impacted critical infrastructure and to ensure that in the event of a disaster that would impact the critical infrastructure that local jurisdictions are aware of potential threats to critical resources in the community. Local hazard mitigation plans should provide a prioritized list of mitigation projects throughout the jurisdiction to be funded as resources are available. In like manner, the state hazard mitigation plan should ensure that critical infrastructure mitigation projects are prioritized in a way that provides the highest level of safety and continuity of operations for critical infrastructure statewide.

Recommendation 6: State and Local Disaster Recovery plans should include priority restoration schedules for critical infrastructure to ensure that appropriate resources are assigned to recover those facilities first after a disaster.

The restoration of critical infrastructure, and especially Community Lifelines, is critical to the recovery of every community. Response and recovery efforts should prioritize these facilities for recovery in the initial stages.

Objective 5: Build support for funding of the critical infrastructure protection plans by gathering and sharing data as well as educating the general public and key stakeholder groups

Discussion

The protection and hardening of critical infrastructure and utilities is a shared responsibility between the public and private sectors. There is an immediate need for closer partnerships between industry and government organizations to foster an aligned infrastructure security system. The creation of CISA serves as a major asset for DHS in promoting public-private partnerships as an increase in funding and autonomy enables the agency to speed up the department's efforts to protect our nation's critical infrastructure.

A significant portion of the state's critical infrastructures is privately owned or operated, meaning that the private sector is initially responsible for providing protection against threats to their facilities. The ultimate goal would allow critical infrastructure owners and operators to initiate plans and procedures that would limit or negate the need for any government assistance due to a disaster and would maintain service to its customers throughout the disaster.

Recommendation 7: Develop public support to provide funding for critical infrastructure resilience projects.

At the local and regional level public and private entities such as cities, counties, councils of government and private critical infrastructure owners, can work together to engage the public and build support for resilience initiatives and funding through a variety of actions including:

- Establishment of Data Sharing Agreements: Data-sharing agreements are needed where resilience issues cross jurisdictional boundaries, and with University experts and other appropriate researchers to develop the information necessary to establish the resilience needs of the communities.
- Data Gathering & Initial Assessment: Work with select communities to access available data, policies and plans to establish an initial picture of community resilience across and between systems and identify key data needs and gaps.
- Develop clear strategies to focus attention and support on resilience efforts that will support the communities as a whole.
- Engagement of the public through informational sessions and media campaigns on community resilience and the need to support these efforts.
- Support P3 Development: Investigate development of public-private-partnerships with locally based industry to advance resilience through existing tools such as the Community Reinvestment Act.
- Expand relationships with local, state and federal elected officials to inform them of the potential threats and hazards facing critical infrastructure and the need to provide funding to limit the impact/effects of a disaster within a community, while building the resilience of these facilities.

Recommendation 8: Develop a comprehensive prioritization methodology for critical infrastructure facilities with a preference for Community Lifelines' that may be used across local, state, and federal programs.

The Department of Public Safety, Office of Homeland Security, Office of Critical Infrastructure Protection the Cybersecurity and Infrastructure Security Agency, and the Texas Division of Emergency Management, together with local jurisdictions and critical infrastructure owners and operators should develop a prioritization framework that can be used by local jurisdictions, and the state and federal governments to aid in the targeting of limited financial resources toward high priority critical infrastructure resilience efforts. This prioritization could provide a focus for mitigation planning and dissemination of funding at all levels. An additional potential outcome from the prioritization effort could include the identification of critical infrastructure of national significance. The facilities of national importance are a key factor in determining the allocation of federal resources for mitigation efforts. Identification of additional facilities of national significance could increase the amount of federal funding that Texas receives for these efforts.

Objective 6: Provide timely information to critical infrastructure owners and operators of potential threats and disasters which may impact their facilities.

Recommendation 9: Notify critical infrastructure owners and operators of potential threats to their operations in a timely manner.

The Texas Division of Emergency Management in coordination with other relevant state agencies should develop communications strategies to share information regarding potential threats and disasters which may affect critical infrastructure and facilities. Owners and operators of these facilities in the public and private sectors could voluntarily sign up for the notification system. When a threat or disaster may affect a facility, TDEM could provide notification to those facilities of the nature and potential impact on the facility to ensure that these facilities may take appropriate steps to protect the facility.

Objective 7: Protect the information regarding critical infrastructure to ensure that these facilities are not targeted for disruption.

Critical infrastructure owner and operator information must be protected to include risk, vulnerability, mitigation, resilience and proprietary information in accordance with all applicable state and national laws and regulations. The level of protection that is provided for this information will be directly related to the level of participation for many sectors of critical infrastructure.

Texas Government Code Sections 418.176, 418.177 and 418.181 protects information related to contact information to be used in the event of a terrorist incident or criminal activity, information related to risk and vulnerability assessments related to terrorism or related criminal activity, and technical details of vulnerabilities of critical infrastructure to terrorism. These statutes provide protection for this information related to terrorism and criminal activity, but information collected for the purposes of assessing risk, planning, response and recovery from man-made and natural disasters could be used in the same manner as the information for terrorism or criminal activity.

Recommendation 10: Include the protection of information related to threats and hazards of natural and man-made disasters to that of terrorism or criminal activity.

Amend Texas Government Code Sections 418.176, 418.177, and 418.181 to include all hazards in addition to terrorism or criminal activity.

Objective 8: Request the Cybersecurity and Infrastructure Security Agency to update the Infrastructure Protection Report Series.

The most recent update to the Critical Infrastructure Report Series occurred in 2013. To ensure that this information is updated to reflect new potential risks and innovative measures to protect against these threats, the updating of these reports would provide beneficial information to critical infrastructure owners and operators.

Recommendation 11: The state of Texas encourages the Department of Homeland Security to update the Critical Infrastructure Report Series.

Objective 9: Encourage proposed Critical Infrastructure Projects to conduct a Critical Infrastructure Risk Assessment of a potential facility location and design prior to construction.

Recommendation 12: Agencies of the state and local jurisdictions should encourage a risk assessment of any proposed critical infrastructure within their oversight as a requirement to permitting and approval of the project.

The development of a risk assessment prior to construction may assist the facilities in making site selections which will protect the critical infrastructure from foreseeable damage.

Steps to Development and Implementation

This section provides a summary of next steps including organizational approval, legislative approval and follow on steps if approved. It should also include resource requirements as identified.

Detailed next steps

Due Date	Objectives	Team Assignments	Status
11/1/2020	Submission to the Legislature		

Reference List

- *Business Plan for Developing a Critical Infrastructure / Key Resources Geographical Database for Connecticut.* http://www.ct.gov/gis/lib/gis/FINAL_Critical_Infrastructure-Key_Resources_Business_Plan_09-23-08.pdf.

- Department of Homeland Security, Cybersecurity and Infrastructure Security Agency. *A Guide to Critical Infrastructure Security and Resilience*. November 19, 2020. https://www.cisa.gov/publication/guide-critical-infrastructure-security-and-resilience.

- Department of Homeland Security, Protective Security Advisor (PSA) Program; Securing the nations critical infrastructure one community at a time. https://www.cisa.gov/protective-security-advisors.

- Department of Homeland Security. 2017. *Strategic Plan on Infrastructure Protection Assessments.* https://www.dhs.gov/sites/default/files/publications/NPPD%20-%20Strategic%20Plan%20on%20Infrastructure%20Protection%20Assessments.pdf.

- Department of Homeland Security; *Commercial Facility Risk Self-Assessment Tool*. http://www.iaem.com/documents/DHS-Commercial-Facility-Risk-Self-Assessment-Tool.pdf.

- Department of Homeland Security, Critical Infrastructure Sectors. https://www.dhs.gov/cisa/critical-infrastructure-sectors

- Department of Homeland Security. *NIPP Supplemental Tool: Implementing a Critical Infrastructure Risk Management Tool.* https://www.cisa.gov/sites/default/files/publications/NIPP-2013-Supplement-Executing-a-CI-Risk-Mgmt-Approach-508.pdf.

- Department of Homeland Security. *Risk Assessments Inform Owner and Operator Protection Efforts and Departmental Strategic Planning*. https://www.gao.gov/products/GAO-18-62.

- *FEMA, Mitigation Case Studies, Hardened First Responder Facility*. https://www.fema.gov/pdf/plan/prevent/bestpractices/hardened.pdf.

- Federal Emergency Management Agency. 2019. *National Response Framework.* https://www.fema.gov/emergency-managers/practitioners/lifelines

- *FEMA, Safer, Stronger, Smarter: A Guide to Improving School Natural Hazard Safety*. https://www.hsdl.org/?abstract&did=802379

- Federal Emergency Management Agency. *Community Lifelines*. https://www.fema.gov/emergency-managers/practitioners/lifelines.

- Institute for Infrastructure and Information Assurance; *A Vulnerability Assessment Methodology for Critical Infrastructure Facilities*; George H. Baker III, Ph.D. https://battleplan.org/wp-content/uploads/2016/03/VulnerabilityFacilityAssessment.pdf.

- Implementing Critical Infrastructure Protection Programs; Homeland Infrastructure Threat and Risk Analysis Center (HITRAC) Analyses. https://itlaw.wikia.org/wiki/Homeland_Infrastructure_Threat_and_Risk_Analysis_Center.

- National Cyber Awareness System. https://us-cert.cisa.gov/ncas/alerts.

- National Infrastructure Protection Plan; Sector-Specific Plans. https://www.dhs.gov/xlibrary/assets/nipp_sctrplans.pdf.

- National Institute for Standards and Technology. *Cybersecurity Framework.* https://www.nist.gov/cyberframework.

- National Research Council 20212. *Disaster Resilience: A National Imperative*. Washington, DC: The National Academy Press. https://doi.org/10.17226.13457.

- Texas A&M Engineering Extension Service, Critical Infrastructure Protection. https://teex.org/pages/program.aspx?catid=459

- Texas Department of Public Safety. 2019. *Texas: Critical Infrastructure Profile.*

- Texas Government Code Section 421.002. HOMELAND SECURITY STRATEGY. https://statutes.capitol.texas.gov/Docs/GV/htm/GV.421.htm

- U.S. Fire Administration; *The Critical Infrastructure Protection Process Job Aid; Emergency Management and Response-Information Sharing and Analysis Center*. https://www.usfa.fema.gov/downloads/pdf/publications/fa-313.pdf.

- United States Government Accountability Office; *CRITICAL INFRASTRUCTURE PROTECTION*. https://www.gao.gov/assets/700/690112.pdf.

- US homeland security related critical infrastructure matters. https://www.ukessays.com/essays/criminology/us-homeland-security-related-critical-infrastructure-matters-criminology-essay.php?vref=1
- U.S. Department of Education; *A Guide to School Vulnerability Assessments*. https://cdpsdocs.state.co.us/safeschools/Resources/USED%20US%20Department%20of%20Education/Vulnerability%20Assessment%20Guide_2008,0.pdf.

For more information, please contact Eric Shuey, Section Chief, Texas Division of Emergency Management at eric.shuey@tdem.texas.gov.

Appendix 1 – Examples of Strategies to Reduce Risk

Protecting Critical Infrastructure Facilities

The following list contains methods that can be used to protect critical infrastructure facilities:

- Investing in physical and cyber risk management products and plans
- Participating in the community's hazard mitigation planning activities
- Engaging in partnerships to implement community risk reduction projects
- Educating employees about *critical infrastructure* security and resilience
- Planning for business continuity
- Sharing threat and incident information
- Reporting suspicious activity
- Exercising the plans

Reducing Risks to Critical Infrastructure Facilities

To make these facilities more resilient requires taking actions that remove risks to physical infrastructure. Examples for reducing risks to buildings includes the following:

- Relocating
- Elevating the building above the base flood elevation (BFE)
- Dry proofing and wet flood proofing
- Using fire-resistant building materials
- Protecting against Electromagnetic Pulse events
- Creating defensible space for wildfire protection
- Improving drainage
- Retrofitting infrastructure
- Conducting streambank stabilization
- Incorporating engineered solutions such as levees and floodwalls

Examples of hardening capital facilities may include:

- Double sleeving water pipes,
- Elevating roadways prone to flooding above base flood elevation (BFE),
- Expanding the capacity of road culverts,
- Removing physical impediments that restrict water flow in rivers and floodplains,
- Elevating heating and air conditioning equipment and generators.
- Increasing channel capacity by increasing culvert capacity or bridge retrofits
- Protecting bridge abutments and footings with armoring and wingwalls;
- Retrofitting of dams, pipelines, bridges, and other facilities to meet current design standards and rules;

Implementation of physical protection programs to mitigate against man-made threats to the facilities may include:

- Security awareness training for all employees
- Developing, implementing and training all employees on a security plan
- Coordinating security plans with local law enforcement

- Information sharing with local, state and federal law enforcement and homeland security partners
- Integrated security systems
- Access control
- Video surveillance
- Perimeter intrusion detection
- Video analytics
- Physical security information management

Improving Network Cyber Security

One area of mitigation that is frequently overlooked in the development of Critical Infrastructure Protection Plans is that of information security. With the increasing prevalence of cyber-attacks on critical infrastructure, owners and operators must take this factor into consideration in a CIPP. There are many common best practices for hardening networks against cyber threats. The National Institute for Standards and Technology (NIST) created a Voluntary Cybersecurity Framework for protecting critical infrastructure from cyber threats. The Framework provides standards, guidelines, and practices to help owners and operators manage cybersecurity threats to their facilities. Critical Infrastructure owners and operators should review the framework and implement where appropriate to their operations.

The Department of Homeland Security, Cybersecurity and Infrastructure Security Agency (CISA) and the Federal Bureau of Investigations (FBI) also develop recommendations and publish them regularly through the National Cyber Awareness System. It is critical for the development of information security planners to actively review the ever-changing landscape of potential threats. Examples of some of the previous recommendations that have been made include:

- Block the web-based Distributed Authoring and Versioning (WebDAV) protocol on border gateway devices on the network
- Monitor VPN logs for abnormal activity (e.g., off-hour logins, unauthorized IP address logins, and multiple concurrent logins)
- Segment any critical networks or control systems from business systems and networks according to industry best practices
- Establish a password policy to require complex passwords for all users
- Ensure that accounts for network administration do not have external connectivity
- Ensure that network administrators use non-privileged accounts for email and internet access
- Use two-factor authentication for all authentication, with special emphasis on any external-facing interfaces and high-risk environments (e.g., remote access, privileged access, and access to sensitive data)

Additional information related to the types of protection that should be implemented at individual facilities may be obtained from the U.S. Department of Homeland Security, Cybersecurity and Infrastructure Security Agency (CISA) and the Texas Department of Public Safety Office of Critical Infrastructure Protection.