Texas Governance and Authorities for Cyberattack Response: A Summary

By

Amelia A. Boylan

Audrey N. Tepe

Danny W. Davis, Ph.D.

October 31, 2019

INTRODUCTION

This paper outlines the statutory and legal authorities that guide the preparation and response to cyber-type attacks against local and state agencies and private sector entities in Texas. The scope of the threat is identified through the recent ransomware attacks on Jackson County, Texas, the city government of Baltimore, Maryland, the Louisiana School Systems, and the city government of Atlanta, Georgia.

This study does not include any changes to the State response mechanism since the recent ransomware attacks of August 2019. Those cyberattacks were launched against managed service providers (MSP) in Texas and Wisconsin. State responders, aided by federal authorities, responded to the attacks, but no information has been released as of this writing. "Sodinokibi was the [ransomware] strain used in the attack on TSM Consulting Services that encrypted the computers of 22 Texas municipalities, leaving them unable to fulfill tasks such as accepting online payments for water bills, providing copies of birth and death certificates and responding to emails" (Dudley, 2019). This report will be updated as more information on the August incidents becomes available.

The discussion of statutory and legal authority considerations in this paper is divided into three areas:

1. The authorities that direct the preparation for incident response and cybersecurity at both the Federal and State levels,
2. The authority that guides response efforts for emergency management and cyber-attacks in Texas,
3. And the responsibilities of private entities in response to a cyber incident.

Finally, a brief review of the Texas Emergency Response plan is given, and recommendations are made in five areas: state legislative changes, state policy actions, operational methods to address shortfalls, recommended coordination with the federal government, and recommended guidance for private sector companies.

SCOPE OF THE POSSIBLE THREAT

Jackson County, Texas

In May 2019, Jackson County computers and digital records were held ransom by a cyberattack. The County Judge has acknowledged that the County Sheriff, District Attorney, District Clerk, and other offices were affected (Theophil 2019). The hackers demanded a ransom payment in Bitcoin. Jackson County assumes that access was gained using an email phishing attack (Theophil 2019). Even Jackson County's backup data was compromised with unsuccessful attempts to restore it by outside experts (Theophil 2019). Restoration is still ongoing, with costs

exceeding $50,000. Jackson County was assisted in response by a Joint Cyber Incident Response Team from the Texas Military Department. (Texas Military Department 2019) The County Judge intends to implement a cyber insurance policy similar to the one implemented by the neighboring Victoria County in 2018 (Theophil 2019).

City of Baltimore, Maryland

In early May of this year, the City of Baltimore was hit with a phishing attack that used ransomware (Uria 2019). Most, if not all, of the online aspects of running the city were compromised, including government emails, payments to city departments, and real estate transactions (Sullivan 2019). The ransomware attack has cost Baltimore more than $18 million, with $10 million to restore the systems and $8 million in lost revenue, and the recovery is still ongoing (Uria 2019). The hackers demanded a ransom in Bitcoin, but the city refused to pay (Sullivan 2019). The weak link that allowed Baltimore to be compromised was their reliance on old hardware and old software.

Louisiana School Systems

In late July 2019, the Governor of Louisiana declared a state of emergency after cyberattacks compromised at least three school districts (Gagliano 2019). The statewide declaration and recovery are still ongoing. The encrypted and locked data was held for ransom, and payment was requested in bitcoin (Pietri-Freeman 2019). In response, the phones were disabled, and internet services terminated as a precautionary measure. Along with these measures, the state-issued guidance to the school districts on a multiphase plan to prevent a security breach that included the use of an anti-virus program and traffic monitoring system (Gagliano 2019). The Governor's emergency declaration allowed the activation of Louisiana's Emergency Support Function 17, a cyber incident response team, as well as experts from the National Guard and the Louisiana State Police (Holcombe 2019). This team was created in 2017 and is "part of the Louisiana Cybersecurity Commission, a statewide partnership of public, private, academic and law enforcement stakeholders with the expertise to respond to cybersecurity threats" (Gagliano 2019).

City of Atlanta, Georgia

On March 22, 2018, the City of Atlanta acknowledged that a SamSam ransomware attack disrupted five of the 13 local government departments. The resultant critical infrastructure impacts were crippled court services and utilities, including water payment and sewage management, deleted legal documents, and impaired operation of the Atlanta Police Department (Newman 2018). The locked files and internal systems were held at a ransom of $50,000 in bitcoin (Easter et al. 2019, p.31). Atlanta ultimately paid $2.6 million in emergency contracts in attempts to recover with incident response and digital forensics, extra staffing, crisis communications systems, and incident response consulting (Newman 2018). The total cost to the city is over $17 million (Sullivan 2019). The attack left city employees without computers for

five days and brought the entire operation of this hub for transportation, health, and economics to a standstill (Easter et al. 2019, p.32). This attack is the "largest successful breach of security for a major American city by ransomware and affected up to 6 million people" (Easter et al. 2019, p.32). The lack of preparedness resulted in a significant amount of downtime because basic security tenets were not implemented, primarily due to a lack of resources (Newman 2018). The reality from this attack on the City of Atlanta is that a lack of security practices, and motivation to implement them, allowed the City to become vulnerable to this attack.

Additional Threats

Potential threats from cyberattacks are not limited to the types of ransomware attacks as discussed above. Ultimately, cyberattacks can target critical infrastructure areas such as the petrochemical industry, the healthcare industry, election data, and the power grid to identify a few. In 2015, the Ukrainian power grid was hacked, which resulted in 225,000 customers without power for several hours (Easter et al. 2019, p.31). This attack was the first publicly-acknowledged cyberattack that was a direct result of a targeted attack on SCADA systems within a nation's critical infrastructure (Easter et al. 2019, p.32). As of late 2018, 24% of the ransomware Samsam's targets have been hospitals, with more than half of those occurring in the U.S. (Bryant 2018). Healthcare is a popular target because most organizations rely on legacy equipment and fail to install patches or updates, which leaves patient health records and all of their personal data vulnerable to attacks (Bryant 2018). In 2017, the ransomware attacks WannaCry and NotPetya, shut down healthcare services in the U.K., impaired the logistics operations of a shipping giant, and affected the production of the HPV vaccine by the drug maker Merck (Fazzini 2019). WannaCry was attributed to North Korea, and NotPetya to the Russian military, all emphasizing the threat posed by adversarial nation-states. Texas will remain a target for these attacks with the magnitude of critical infrastructure it houses.

The recent cyberattack on Texas demonstrates the crucial pieces that small towns and counties play in the state's cybersecurity. Small towns are more vulnerable due to the lack of available budget to afford large information technology departments, which means they outsource. Outsourcing means managed service providers use the same software and the same applications for all of the government offices they serve (Fazzini 2019).

CURRENT LEGISLATION

Preparedness

Presidential Policy Directive 21 (PPD-21) instructs an amended National Infrastructure Protection Plan (NIPP) (U.S. Department of Homeland Security 2013). The NIPP also integrates the objectives of Executive Order (EO) 13636, Improving Critical Infrastructure Cybersecurity, which promotes information sharing and collaboration between critical infrastructure stakeholders and the federal government (U.S. Department of Homeland Security 2013). The

NIPP establishes a "comprehensive risk management framework and clearly defines critical infrastructure protection roles and responsibilities for... Federal, State, local, tribal, and private sector security partners" (U.S. Department of Homeland Security 2006). EO 13636 also established the National Institute of Standards and Technology (NIST). NIST provides public and private entities with cybersecurity standards, guidelines, and best practices (National Institute for Standards and Technology 2019). For example, the privately-owned Electric Reliability Council of Texas (ERCOT) utilizes the NIST framework to identify and mitigate threats against critical infrastructure (Electric Reliability Council of Texas, n.d.).

Cybersecurity measures have been a pressing issue during Texas legislative sessions as legislators realize the state's continued "reliance on legacy hardware and software systems dating back to the 1980s" (Benton 2019). In the 2017 Legislative session, House Bill (HB) 8, the Texas Cybersecurity Act, was filed and subsequently became law. The Texas Cybersecurity Act establishes "specific measures to protect sensitive and confidential data and maintain cyberattack readiness" (Benton 2019). HB 8 also establishes an Information Sharing and Analysis Center to "provide a forum for state agencies to share information regarding cybersecurity threats, best practices, and remediation strategies" (TX HR 8, 85th Legislature). The Information Sharing and Analysis Center is anchored in Texas Government Code §2054.0594.

The Texas Government Code Chapter 2054 also establishes other significant aspects of the preparedness authority for cybersecurity. Texas Government Code §2054.059, *Cybersecurity*, establishes that a department will "establish and administer a clearinghouse for information relating to all aspects of protecting the cybersecurity of state agency information" and develop strategies and framework for securing cyber infrastructure by state agencies, including critical infrastructure and cybersecurity risk assessments and mitigation planning (Texas Government Code, Chapter 2054 §059). This section also identifies that departments will "develop and provide training to state agencies on cybersecurity measures and awareness" and "promote public awareness of cybersecurity issues" (Texas Government Code, Chapter 2054 §059). In §2054.0591, a cybersecurity report is mandated, in the even-numbered years, that will identify "preventive and recovery efforts the state can undertake to improve cybersecurity in this state" (Texas Government Code, Chapter 2054 §0591). The report must include: "(1) an assessment of the resources available to address the operational and financial impacts of a cybersecurity event; (2) a review of existing statutes regarding cybersecurity and information resources technologies; (3) recommendations for legislative action to increase the state's cybersecurity and protect against adverse impacts from a cybersecurity event; (4) an evaluation of the costs and benefits of cybersecurity insurance; and (5) an evaluation of tertiary disaster recovery options" (Texas Government Code, Chapter 2054 §0591).

The Texas Government Code Chapter 2054, Subchapter E, §2054.091 establishes the preparation of the state strategic plan for information resources management. Section 2054.092 outlines the

content of the plan, which includes identifying "major issues faced by state agencies related to the acquisition of computer hardware, computer software, and information resources technology services and develop a statewide approach to address the issues, including: (A) developing performance measures for purchasing and contracting; and (B) identifying opportunities to reuse computer software code purchased with public funds" (Texas Government Code, Chapter 2054 §0592).

Section 2054.133 identifies the creation of each state agency's Information Security Plan in order to protect the security of the agency's information. The submission of every state agency's plan is due to the Department of Information Resources (DIR) every even-numbered year. This plan includes the consideration of "identify risk management and other measures taken to protect the agency's information from unauthorized access, disclosure, modification, or destruction" (Texas Government Code, Chapter 2054 §133). From the review and receipt of these plans, DIR is responsible for submitting a report to the "governor, the lieutenant governor, and the legislature evaluating information security for this state's information resources" on odd-numbered years (Texas Government Code, Chapter 2054 §133).

Chapter 418 of the Texas Government Code is also known as the Texas Disaster Act of 1975 and establishes preparedness authority. Chapter 418 states that "Each local and interjurisdictional agency shall prepare and keep current an emergency management plan for its area providing for disaster mitigation, preparedness, response, and recovery" (Texas Government Code, Chapter 418 §106). Texas Government Code Chapter 418 also created the Texas Division of Emergency Management (TDEM) as a division of the Texas Department of Public Safety. The duties assigned to the Texas Division of Emergency Management include ensuring unification among the state's emergency management and homeland security approaches and maintaining a state emergency management plan (Texas Government Code, Chapter 418). While this disaster recovery Act encompasses mitigation, preparedness, response, and recovery, it fails to address cybersecurity specifically.

Texas Government Code Chapter 421 outlines Texas law relating to homeland security. This statute outlines the Governor's responsibility to "coordinate homeland security activities among and between local, state, and federal agencies and the private sector and must include specific plans for: … detecting, deterring, and defending against terrorism, including cyber-terrorism and biological, chemical, and nuclear terrorism" (Texas Government Code, Chapter 421 §002(b)). This chapter also establishes special advisory committees and annual homeland security reports.

The 86th (2019-2020) Legislature enrolled House Bill 3834, "relating to the requirement that certain state and local government employees and state contractors complete a cybersecurity training program certified by the Department of Information Resources" (Texas HR 3834, 86th Legislature). The bill requires DIR to "certify at least five cybersecurity training programs for

state and local government employees; and update standards for maintenance of certification by the cybersecurity training program under this section." This new standard will be codified in Texas Government Code Section 2054.519.

In the Texas Administrative Code, Part 10 Department of Information Resources, Chapter 202 establishes Information Security Standards and provides direction for preparedness for cyber incidents to specific agencies and universities. Section 202.21 directs the position of an Information Security Officer (ISO) and their responsibilities (this requirement is also mandated under Texas Code §2054.136). ISO's develop and maintain an information security plan as required by §2054.133 of the Texas Government Code and coordinate and review other data security requirements (Texas Administrative Code, §202.21).

Section 202.22 delegates the staff responsibilities as "Information owners, custodians, and users of information resources shall, in consultation with the agency IRM and ISO, be identified, and their responsibilities defined and documented by the state agency" (Texas Administrative Code, §202.22). Section 202.26 requires the development of a security control standards catalog and establishes the minimum requirements for security controls (Texas Administrative Code, §202.26). It also establishes that in order for the DIR to develop new standards, specific requirements must be met, with one including the necessity to "(3) minimize the impact to an affected agency, to the extent possible by: (A) ensuring that such standards and guidelines do not require the use or procurement of specific products, including any specific hardware or software; (B) ensuring that such standards provide for flexibility to permit alternative solutions to provide equivalent levels of protection for identified information security risks; and (C) using flexible, performance-based standards and guidelines that permit the use of off-the-shelf commercially developed information security products" (Texas Administrative Code, §202.26). Lastly, it allows the application of more stringent standards where the "head of an agency may employ standards for the cost-effective information security of information and information resources within or under the supervision of that agency that are more stringent than the standards the department prescribes under this section if the more stringent standards: (1) contain at least the applicable standards issued by the department; or (2) are consistent with applicable federal law, policies and guidelines issued under state rule, industry standards, best practices, or deemed necessary to adequately protect the information held by the agency" (Texas Administrative Code, §202.26).

Executive Orders of the Governor that establish preparedness authority include RP32, as a base document for GA05, and GA05. 'Relating to Emergency Management and Homeland Security, RP-32' establishes the Emergency Management Council and designates the members, charges the Governor's Division of Emergency Management to "exercise the powers granted" to the Governor under the Texas Disaster Act of 1975 (Chapter 418 of the Texas Government Code), and establishes "Disaster Districts" (Perry 2004). 'Disaster Districts' establish committees

consisting of district representatives to report to the Office of Homeland Security on matters relating to emergencies and disasters (Perry 2004). The State Emergency Response Commission (SERC) is also mandated to be a standing element of the Emergency Management Council "in order to carry out certain state emergency planning, community right-to-know, and response functions relating to hazardous materials" (Perry 2004). This order also designates that "mayors and county judges shall serve as the Governor's designated agents in the administration and supervision of the Act, and may exercise the powers, on an appropriate local scale, granted the Governor therein" (Perry 2004). It also permits each mayor and county judge to select an Emergency Management Coordinator for their political subdivision (Perry 2004).

'Relating to Emergency Management of Natural and Human Caused Events, Emergencies, and Disasters, GA-05' alters the members of the Emergency Management Council and the SERC (Abbott 2018). GA-05 emphasizes that "in compliance with Texas Government Code, Section 418.101, the presiding officer of each political subdivision shall promptly notify the Chair of the manner in which it is providing or securing an emergency management program, and of the person designated to head that program, by February 1 of each year" (Abbott 2018).

Response

The National Response Framework (NRF) "describes the principles, roles and responsibilities, and coordinating structures" that govern incident response measures in the United States (U.S. Department of Homeland Security 2016b). The NRF identifies mitigating cybersecurity threats and incidents as a component of the National Preparedness Goal and a core capability of the NRF. The NRF assigns the responsibilities of commanding state military forces (National Guard) to the Governor of a state. When the National Guard is operating under Title 32 of U.S. Code or State Active Duty, they are under the direction of the Governor (National Guard 2006).

Presidential Policy Directive 41 (PPD-41) directed the establishment of a National Cyber Incident Response Plan (NCIRP) (U.S. Department of Homeland Security 2016a). The NCIRP establishes guiding principles for the roles of the Federal Government, state and local governments, and private entities in responding to cyber incidents (U.S. Cybersecurity and Infrastructure Security Agency, 2019). The NCIRP "serves as the primary strategic framework for stakeholders to understand how federal departments and agencies and other national-level partners provide resources to support response operations" (U.S. Department of Homeland Security 2016a p.4). In the aftermath of a cyber incident, the NCIRP intends to advise state and local governments of the federal and national-level resources available to them (U.S. Department of Homeland Security 2016a p.7). The NCIRP states that each state is responsible for developing plans that "describes their role in asset response for entities within their state" (U.S. Department of Homeland Security 2016a, p.16). The state plan should be consistent with the NCIRP and serve as a cyber annex to their respective state emergency plan; the NCIRP offers information for each state to consider when developing a cyber incident response plan that "coordinates

identifying, detecting, mitigating, responding to, and recovering from cyber incidents in their state" (U.S. Department of Homeland Security 2016a, p.16).

Both the NRF and the NCIRP structures align with The National Incident Management System (NIMS) in response efforts. NIMS "provides the common language and incident management structure for government at all levels (federal and SLTT) and the private sector and defines standard command and management structures" (U.S. Department of Homeland Security. 2016a, p.9). In a cyber incident, NIMS helps provide the ability to share resources, coordination, and communication of information which are essential for a successful cyber response effort (U.S. Department of Homeland Security 2016a, p.9). In Executive Order from the Governor RP-40, 'Relating to the Designation of the National Incident Management System as the Incident Management System for the State of Texas,' then-Governor Rick Perry identified NIMS as the ultimate guidance for Texas' incident management (Perry 2005).

Along with amending the National Infrastructure Protection Plan, PPD-21 assigns a Federal department or agency to each critical infrastructure sector. The sector-specific agencies are assigned multiple responsibilities, including to "provide, support, or facilitate technical assistance and consultations for that sector to identify vulnerabilities and help mitigate incidents, as appropriate" (Obama 2013). PPD-21 assigns the Department of Justice as lead on "counterterrorism and counterintelligence investigations and related law enforcement activities across the critical infrastructure sectors" (Obama 2013). Presidential Executive Order 13800 also assigns the Department of Justice, specifically the Federal Bureau of Investigations, to investigate cyber incidents and assign attribution (Trump 2017).

The Robert T. Stafford Disaster Relief and Emergency Assistance Act (Stafford Act) dictates that "all requests for a declaration by the President that a major disaster exists shall be made by the Governor of the affected State" (42 U.S. Code §5170). Chapter 433 of the Texas Government Code reiterates the responsibility of the Governor to "proclaim a state of emergency and designate the area involved" (Texas Government Code, Chapter 433). Chapter 418 of the Texas Government Code and Title 37, Chapter 7 of the Texas Administrative Code allow "mayors and county judges" to "serve as emergency management directors, bearing the responsibility for maintaining an emergency management program within their respective jurisdictions" (Texas Administrative Code, Title 37, Chapter 7).

House Bill (HB) 9, the Texas Cybercrime Act, was filed and later became law during the 2017 Legislative session. The Texas Cybercrime Act "updates the Texas Penal Code to recognize several new types of cybercrime and their punishments" (Benton 2019). This bill encourages the pursuit of cybercrimes by law enforcement.

The Texas Government Code establishes a few response authority procedures for a cyber-related event. Section 2054.0592 establishes a way to request cybersecurity emergency funding. “If a cybersecurity event creates a need for emergency funding, the department may request that the governor or Legislative Budget Board make a proposal” to “provide funding to manage the operational and financial impacts from the cybersecurity event” (Texas Government Code, Chapter 2054 §0592).

Another section of the Texas Government Code, §2054.1125: Security Breach Notification by State Agency, establishes the only found response protocol. It ultimately establishes that within 48 hours of a breach of system security, a notification must be given to DIR or, if election data is involved, the Secretary of State (Texas Government Code, Chapter 2054 §1125). Nested within this section is a reference to the Business and Commerce Code §521.002 and §521.053, which defines essential aspects within the Texas Government Code. Within the Business and Commerce Code, the definitions of “breach of security system” and “sensitive personal information” is found and the notification requirements are identified (Texas Government Code, Chapter 2054 §1125). The notification requirements are ultimately for those individuals who had or possibly had their information compromised (Texas Business and Commerce Code §521.053).

Response authority from Executive Orders of the Governor can be found in ‘Relating to Implementing Recommendations from the Governor’s Task Force on Evacuation, Transportation, and Logistics, RP-57.’ Most of the executive order discusses hurricane evacuation protocol after the Hurricane Rita evacuation in 2005. In the section labeled “Command, Control, and Communications” it is decided that the “Emergency Management Directors (County Judges and Mayors) within each of the state’s 24 Councils of Government shall establish a Regional Unified Command Structure (RUCS) and appoint a single Incident Commander for the Regional Unified Command Structure. Each Regional Unified Command Structure will be responsible for preparing for and responding to catastrophic events within the region. Each Incident Commander will be the operational commander within the region during a disaster response, including a mass evacuation” (Perry 2006).

Local and county authorities for cyber incidents are found in the Texas Government Code Chapter 418.102. This section indicates that each county shall maintain an emergency management program that provides and serves its entire jurisdictional area (Texas Division of Emergency Management 2019a p7). The Texas Emergency Management Executive guide continues to say that the “emergency management program of a county must be coordinated with the emergency management programs of municipalities situated in the county but does not apply in a municipality having its own emergency management program” (Texas Division of Emergency Management 2019a p7).

The Texas Administrative Code, in Title 37, Chapter 7, rule §7.1 directs that each incorporated city in Texas shall maintain an emergency management agency or participate in a local or inter-jurisdictional emergency management agency (Texas Division of Emergency Management 2019a p7). Also, according to Title 37, Chapter 7, Rule §7.12, jurisdictions must prepare emergency operations plans (EOP) that follow the Texas Department of Emergency Management's (TDEM) planning standards. Furthermore, each local and inter-jurisdictional emergency management agency has the following planning-related responsibilities: (1) Prepare an EOP that includes the minimum content described in TDEM's planning standards; (2) Obtain the signature(s) of the presiding officer(s) of the jurisdiction(s) on the plan; (3) Local and inter-jurisdictional plans shall be reviewed annually and must have been prepared or updated during the last five years to be considered current; and (4) A copy of each plan and any changes will be provided to TDEM (Texas Division of Emergency Management 2019a p7).

Private Industry Responsibilities

According to the NCIRP, Private sector "entities perform critical roles in supporting threat response activities by reporting and sharing information regarding cyber incidents and malicious cyber activity in a timely manner to appropriate law enforcement agencies or government entities" (U.S. Department of Homeland Security 2016a, p.12). The NCIRP also states that "private sector cybersecurity practitioners and providers that offer critical services (such as managed security services, indications and warning, cybersecurity assessment, and incident response) may also possess information concerning malicious cyber activity that is important to enable threat response activities" (U.S. Department of Homeland Security 2016a, p.12). Through the Cybersecurity Information Sharing Act of 2015, critical legal protections and conditions are established regarding sharing information with the Federal Government, state and local governments and the private sector (U.S. Department of Homeland Security 2016a, p.13).

The incorporation of the private industry into state organizations and councils to advise and assist on cyber-related matters has been seen through the initial development of the Texas Cybersecurity, Education, and Economic Development Council (TCEEDC) and its successor, the Texas Cybersecurity Council. In 2011, the 82nd Texas Legislature passed, and the Governor signed Senate Bill (SB) 988, which authorized the interim creation of the Texas Cybersecurity, Education, and Economic Development Council. This Council was a mix of government, academia, and industry that examined the state's "cybersecurity infrastructure, its cybersecurity industry, and the cybersecurity educational needs for fostering a vigilant and effective cyber culture" (Texas Cybersecurity, Education, and Economic Development Council 2012, p.1). The Council ultimately found that the focus should include "Texas business and public leaders in collaborative efforts to identify and mitigate risks and threats to Texas citizens and to spur innovation in the cyber environment" (Texas Cybersecurity, Education, and Economic Development Council 2012, p.1). The Council made ten recommendations for the state of Texas. The Texas Cybersecurity, Education, and Economic Development Council was abolished in

2013 in accordance with Senate Bill 988, but its successor became the Texas Cybersecurity Council and was established as follows.

The Texas Government Code also mentions the private industry in §2054.511 when it authorizes the Executive Director of DIR to designate a Cybersecurity Coordinator, which was modified from the Texas Senate Bill 1102 from the 83rd Legislature Regular Session. The Cybersecurity Coordinator was given the authority to "establish a private industry-government council under sections 2054.512 and to utilize the council to implement the recommendations and initiatives under section 2054.514" (Texas Department of Information Resources 2019). The DIR created the Texas Cybersecurity Council with the purpose of developing "enduring partnerships between private industry and public sector organizations to ensure that critical infrastructure and sensitive information are protected, to develop an exemplary cybersecurity workforce to protect technology resources from increasing threats, and develop strategies and solutions that ensure that Texas continues to lead in areas of cybersecurity at a national level" (Texas Department of Information Resources 2019).

Within the Business and Commerce Code, the private sector is mentioned in regard to providing response assistance during a state declared disaster or emergency. Chapter 112, Facilitating Business Rapid Response to State Declared Disasters Act, says that "during those periods of time, out-of-state businesses and employees performing business activities in Texas on a temporary basis solely for the purpose of helping the state recover from a disaster or emergency should not be burdened by any requirements that the out-of-state businesses or employees pay taxes as a result of performing those activities" (Texas Business and Commerce Code §112.005(3)). Section 112.005 states that to "ensure that out-of-state businesses may focus on quickly responding to the needs of Texas and its citizens during a disaster or emergency, it is appropriate for the legislature to provide that those businesses and their employees are not subject to certain state and local registration and licensing requirements and taxes for performing business activities before, during, and after the disaster or emergency to repair and restore devastating damage to critical property and infrastructure in the state" (Texas Business and Commerce Code §112.005).

In the most recent legislative session, two Senate Bills were passed that aim to boost cybersecurity for the Texas electric grid. Senate Bill 475 establishes the Texas Electric Security Council in order to coordinate the sharing and implementation of the best security practices within the industry (Mai 2019). The Texas Electric Security Council will include a governor's appointee, a member of the Public Utilities Commission, and the chief executive officer of Electric Reliability Council of Texas (ERCOT). The Council will be responsible for "developing grid security standards, preparing for grid-related security threats and amending the state emergency plan to ensure coordinated response and recovery efforts" (Mai 2019). Senate Bill 936 creates a framework for collaboration among "state regulators, utilities and the reliability

coordinator to secure grid infrastructure against cyberattacks through a cybersecurity monitor program" (Mai 2019). It ultimately "outlines what cybersecurity 'monitored utility' means" (*Security Magazine* 2019).

TEXAS EMERGENCY RESPONSE PLAN

Chapter 2054 of the Texas Government Code assigned the responsibility of responding to cyberattacks to the Texas Department of Information Resources (DIR) (Texas Government Code, Chapter 2054). This responsibility is carried out by DIR's Texas Cybersecurity Council. This Council aims to develop private-public partnerships in order to protect critical infrastructure and information, grow the cybersecurity workforce, and expand cybersecurity-related strategies and solutions (Texas Department of Information Resources 2019).

Texas' emergency response plan is directed by the preparedness and response legislation outlined in the previous section. The authorities for a cybersecurity emergency are generally outlined by federal and state laws, policies, and mandates. Information, best practices, and other resources are provided by entities such as NIST and the Texas Cybersecurity Council. However, a publicly available, detailed document containing all authorities and procedures for responding in an emergency, specifically a cybersecurity emergency, was not found while researching this topic.

Texas Military Department. The Texas Military Department's cyber mission is to "provide the Governor and the President with mission-ready cyber forces in support of state and federal authorities." (Texas Military Department 2019 2) The entities within the Texas Guard's Cyber Force structure are the State of Texas' Cyber Incident Response capabilities, which are scalable to the response necessary and begin at the local level. These forces include a Defensive Cyber Operations Element (DCOE), Air Force National Guard 273rd Cyber Operations Squadron, Army National Guard Cyber Protection Team 178, and the Texas State Guard Cyber Team. These 'Cyber Mission Packages' (1) "Conduct assessment, mitigation and incident response for state cyber incidents," (2) "Provide Train, Advise and Assist Teams," and (3) "Coordinate with Mission Partners to improve cybersecurity unity of effort." (Texas Military Department 2019 5)

In May 2019, the TMD deployed a Joint Cyber Incident Response Team after Jackson County declared a State of Emergency (first cyber declaration in Texas). The Joint Cyber Incident Response Team assisted Jackson County for 15 days "to restore critical services, establish a stable and robust network, get users back online with updated systems, set up an enumerated network with the latest security patches and develop a clear path ahead for improved cybersecurity practices." (Texas Military Department 2019 7) After the August Ransomware attacks, seven Joint Cyber Incident Response Teams were deployed to assist in the response effort in seven municipalities. The Teams provided on-site cyber incident response support to

include “cyber liaison support to the State Operations Center and operational support to the TMD Joint Operations Center.” (Texas Military Department 2019 8)

REMEDIATION AND RECOVERY RECOMMENDATIONS

State Legislative Changes:

House Bill 3834, “relating to the requirement that certain state and local government employees and state contractors complete a cybersecurity training program certified by the Department of Information Resources” was recently passed in the 86th Legislative session (Texas HR 3834, 86th Legislature). HB 3834 aids in establishing training requirements for key personnel involved with state and local government. The bill requires DIR to certify and update standards for maintaining certification for a minimum of five cybersecurity training programs. HB 3834 is beneficial because it recognizes the importance of cybersecurity training and identifies suitable training for government employees and contractors. However, these standards do not adequately dictate the specific cybersecurity standards that government employees and contractors should possess.

Texas legislation, such as HB 3834, uses vague language and should include more specific guidance for state and local governments. DIR’s responsibility should be expanded to include defining the necessary cybersecurity awareness education that employees should possess to improve cybersecurity capabilities of government employees and contractors. This expansion of responsibilities should include knowledge regarding potential threats, relevant software, and cybersecurity response. DIR should review and update these standards each year to ensure they are up to date with current cybersecurity knowledge. Since cybersecurity is a continually evolving field, legislation should designate an agency to review and update standards rather than dictate standards within the law.

State Policy Actions:

Improved Cyber Incident Response Framework and Plan. Laws have assigned the roles and responsibilities of federal and state agencies in response to a cyber incident. Texas has also created a Texas Cybersecurity Strategic Plan (Texas Department of Information Resources 2018). However, this plan is vague and does not establish a specific emergency response plan and operational guidelines that can be implemented by state and local agencies.

The Texas Department of Emergency Management (TDEM) needs to develop a detailed cyber incident emergency response plan in accordance with the cyber incident response plan used by Department of Homeland Security and cybersecurity framework provided by NIST (U.S. Department of Homeland Security 2016a). This plan should include operational guidelines for preparation, detection and analysis, response and recovery, and repairs to prevent another, similar cyber incident. It should serve as a single, comprehensive resource that consists of the

established roles and responsibilities, operational guidelines, relevant laws and statutes, notification requirements, and templates to aid local agencies in reporting and responding to cyber incidents. This comprehensive resource would enhance uniformity among federal, state, and local cyber response efforts, which would improve collaboration and mutual comprehension of operating procedures. TDEM should then provide local agencies with templates based on the state cyber incident response plan to inform local policies and implement the response plan at all levels.

Additionally, Texas needs to align itself with federal and neighboring states and jurisdictions in its cyber response to ensure consistency in response plans and legislative standards, which is beneficial if a company or agency experiences a breach that impacts individuals from other states and jurisdictions. This alignment simplifies the response process, aids collaboration, and minimizes losses for companies (who, otherwise, may have to hire lawyers for each affected state).

Cyber Insurance. Houston and Dallas are two of Texas' cities that have invested in cyber insurance coverage. Cyber insurance covers "expenses related to security breaches in the city's network, including crisis response, recovery of losses and answers to legal claims stemming from cyberattacks" (Ketterer 2018). Cyber insurance is a valuable asset for cities to have because it significantly helps a city re-stabilize and recover after a cyber incident. Though cities should prepare for cyber incidents and minimize vulnerabilities, it is impossible to be entirely secure. In instances where prevention methods fail, cyber insurance can alleviate the financial burden accompanying a cyber incident. Texas should encourage cities to participate in cyber insurance individually or offer cyber insurance coverage through statewide insurance or mutual aid.

Operational methods that could address shortfalls:

Mutual Aid. A cybersecurity mutual aid system, similar to the Texas Intrastate Fire Mutual Aid System (TIFMAS), could be adopted in order to ensure that Texas is prepared and has trained personnel available to respond to a cyber incident (Texas Interagency Coordination Center 2019). A statewide cyber response team could consist of a variety of specialists who train at information gathering, information analysis, and recovery. This system would help assign attribution, aid agencies in recovery, and restore critical infrastructure when necessary. A mutual aid system could distribute grant funds and ensure that there is an established and organized response when a cyber incident occurs. Texas could also offer cyber insurance for cities and counties as an incentive to opt into the mutual aid system.

Cybersecurity Oversight Committee. There should be an oversight committee assigned to ensuring that agencies' cybersecurity is adequate to include investing in software updates for state and local agencies and ensuring that those agencies are implementing those updates. Updates are crucial because Texas' critical infrastructure, including pipelines and hydroelectric

dams, is currently dependent on vulnerable technology such as SCADA. SCADA is the same technology that was breached by a Syrian hacktivist group in order to hack into a water treatment plant in 2016. This 2016 cyberattack revealed the "clear need to invest in intrusion detection, prevention, patch management and analytics-driven security measures" (Leyden 2016). This breach could have caused damage to property and civilians and displays the vital role cybersecurity has in regard to critical infrastructure.

Training and Preparedness Exercises. To improve cybersecurity knowledge within the government, the Texas Department of Information Resources should establish a standard for cyber training criteria for all government employees. Elected officials and senior officials should have required training for their positions due to the accessibility and range of sensitive information they may have access to while at work.

Once a comprehensive cyber incident response plan is established in Texas, preparedness exercises should be conducted to identify areas for improvement and practice implementation of the plan. The Armed Forces Communications & Electronics Association (AFCEA) hosted Jack Voltaic 2.0, a preparedness exercise that included members of government and critical infrastructure partners (Army Cyber Institute 2018). The exercise introduced participants to a hypothetical scenario in which a cyber incident impacted critical infrastructure. Participants at the operational level, mid-level management, and senior executive level participated in conducting a response to resolve the scenario (Army Cyber Institute 2018). This exercise allowed participants to practice collaboration between the private and public sectors, cyber-related decision-making, and execution of federal cyber response procedures. Conducting a similar exercise state-level exercise that includes senior officials in government and critical infrastructure personnel could significantly improve Texas' cyber incident response.

Intelligence Sharing. Texas should focus on growing and improving the Information Sharing and Analysis Center established by HB 8. An effective state-level intelligence cell or fusion center could help centralize mitigation efforts and intelligence sharing. The state of New Jersey has a New Jersey Cybersecurity & Communications Integration Cell (NJCCIC). The NJCCIC is a "one-stop shop for cybersecurity information sharing, threat analysis, and incident reporting" that works to make New Jersey "more resilient to cyber attacks", as well as, "promote statewide awareness of local cyber threats and widespread adoption of best practices" (New Jersey Cybersecurity and Communications Integration Cell, 2019). The NJCCIC provides resources for citizens, businesses, and government and has a threat center that can monitor cyber threats and share alerts and advisories. Texas should consider adopting similar practices within its Information Sharing and Analysis Center to improve the public's awareness of cybersecurity and establish a centralized location for cyber-related information.

Recommended coordination with the Federal government:
Emergency and Disaster Declarations. The Stafford act permits emergency and major disaster declarations (Texas Division of Emergency Management 2019a). Both types of declarations allow for the President to provide supplemental assistance, such as reimbursements and resources. The Stafford Act refers to Title 6 of the U.S. Code, which relates to domestic security and includes cyber as a type of threat (6 U.S. Code §608). The Stafford Act also states that "a continuous national effort is required to ensure the reliable provision of cyber and physical infrastructure services critical to maintaining the national defense, continuity of government, economic prosperity, and quality of life in the United States" (42 U.S.Code §5195c). The Stafford Act further includes physical and virtual systems and assets in its definition of critical infrastructure and includes cyberinfrastructure and telecommunications infrastructure as systems that could be compromised to harm critical infrastructure.

The Stafford Act recognizes the critical role that cybersecurity plays in public safety and critical infrastructure protection, as do other states that have made emergency declarations for cyber incidents previously (Freed 2019). It is essential that Texas also recognizes cyber incidents as a persisting threat and utilizes emergency and disaster declarations for cyber incidents when necessary. This assistance from the federal government will help ensure that Texas has the resources to fully recover after a cyber incident.

Recommended guidance for private sector companies. Within the private sector, the local chapters of InfraGard should prove to be a reliable resource for Texas and cybersecurity information sharing. In 2005, then FBI director Robert Mueller identified the possibility of this relationship through InfraGard's ability to help the FBI promote the security of computer systems that controlled the nation's critical infrastructure (McKenna 2005). "One example Mueller cited in his remarks involved an InfraGard member in Colorado who alerted FBI agents to the theft of software templates used by energy providers in the United States which hackers could potentially use to penetrate a number of computer systems controlling parts of the nation's energy grid" (McKenna 2005). Another example of state's partnering with InfraGard to explore avenues of cyber incident response occurred in January 2019 when InfraGard Maryland hosted its inaugural Cybersecurity conference. The stated audience includes the state government and law enforcement, and the purpose was "to raise Cybersecurity awareness within the Maryland Community" (Federal Business Council 2019).

CONCLUSION

State and local entities are growing targets for cyberattacks within the U.S., as indicated by the ransomware attacks in Texas in August of this year. The recommendations for the State of Texas include legislative changes, state policy actions to include a cyber incident response framework and cyber insurance, operational methods to include mutual aid, cybersecurity oversight, training

and preparedness exercises, and intelligence sharing, coordination with the Federal government for emergency and disaster declarations, and private sector coordination and partnerships. The implementation of these recommendations can strengthen the preparedness and response capabilities of Texas and decrease the vulnerabilities for future cyber-attacks.

References

Abbott, Greg. 2018. "Executive Order by the Governor of the State of Texas GA05, Relating to Emergency Management of Natural and Human-Caused Events, Emergencies, and Disasters."

Army Cyber Institute. 2018. "Jack Voltaic 2.0: Threats to Critical Infrastructure." https://www.afcea.org/event/sites/default/files/files/JackVoltaic_ExecSummary_R12%20(Final).pdf

Benton, Jackie. 2019. "Cyberdefense for Texas State Government." Comptroller.Texas.Gov. https://comptroller.texas.gov/economy/fiscal-notes/2019/mar/tx-cyberdefense.php

Bryant, Meg. 2018. "Samsam ransomware continues to target hospitals." HealthcareDive.com. https://www.healthcaredive.com/news/samsam-ransomware-continues-to-target-hospitals/541122/

Critical Infrastructures Protection. 42 U.S.Code §5195.

Dudley, Renee. 2019, September 12. The New Target That Enables Ransomware Hackers to Paralyze Dozens of Towns and Businesses at Once. ProPublica. Retrieved from: https://www.propublica.org/article/the-new-target-that-enables-ransomware-hackers-to-paralyze-dozens-of-towns-and-businesses-at-once

Easter, Tiffany, Adam Eaton, Haley Ewing, Trey Green, Chris Griffin, Chandler Lewis, Kristina Milligan, and Keri Weinman. 2019. "Comprehensive U.S. Cyber Framework: Key Aspects of Critical Infrastructure, Private Sector, and Personally Identifiable Information."

Electric Reliability Council of Texas. n.d. "Protecting ERCOT's electric system from cyber attacks." http://www.ercot.com/content/wcm/lists/144927/Cybersecurity_One_Pager_FINAL.pdf

Emergency Management. Texas Government Code, Chapter 418.

Exemption of Out-of-State Employee from Certain Obligations During Disaster Response Period. Texas Business and Commerce Code §112.005.

Fazzini, Kate. 2019. "Texas Ransomware attacks show big gaps in cyber defenses - expect more like them." CNBC. https://www.cnbc.com/2019/08/22/texas-ransomware-attacks-tell-the-us-cybersecurity-story.html

Federal Business Council. 2019. "1st Annual Maryland InfraGard CyberSecurity Conference." https://www.fbcinc.com/e/InfragardCyber/default.aspx

Freed, B. 2019. "Emergency declarations improve cyberattack recovery, report says." *Statescoop.* https://statescoop.com/emergency-declaration-louisiana-cyberattacks-improve-recovery-moodys/

Gagliano, Katie. 2019. "Louisiana School System takes precautions after cyber attack." Center for Digital Education. https://www.govtech.com/education/Louisiana-School-System-Takes-Precautions-After-Cyber-Attack.html

Holcombe, Madeline. 2019. “Louisiana's governor declares an emergency after cyberattacks on several school systems.” CNN.com. https://www.cnn.com/2019/07/25/us/louisiana-schools-cybersecurity-attack/index.html

Homeland Security. Texas Government Code, Chapter 421.

Information Resources. Texas Government Code, Chapter 2054.

Ketterer, Samantha. 2018. “Houston Buys $30M Cyber Insurance Policy.” *Government Technology.* https://www.govtech.com/budget-finance/Houston-Buys-30M-Cyberinsurance-Policy.html

Leyden, John. 2016. “Water treatment plant hacked, chemical mix changed for tap supplies.” *The Register.* https://www.theregister.co.uk/2016/03/24/water_utility_hacked/

Mai, HJ. 2019. “Texas passes first grid protection bills to boost cybersecurity monitoring and best practices.” Utility Dive. https://www.utilitydive.com/news/texas-passes-first-grid-protection-bills-to-boost-cybersecurity-monitoring/555386/

McKenna, Corey. 2005.” InfraGard Critical Resource for Cybersecurity, FBI Director Says.” *Government Technology*. https://www.govtech.com/security/InfraGard-Critical-Resource-for-Cybersecurity-FBI.html

National Guard. 2006. “National Guard Fact Sheet.” https://www.nationalguard.mil/About-the-Guard/Army-National-Guard/Resources/News/ARNG-Media/FileId/137011/

National Guard. 32 U.S. Code.

National Institute for Standards and Technology. 2019. “Cybersecurity.” Information Technology. https://www.nist.gov/topics/cybersecurity

National Institute for Standards and Technology. 2019. “Cybersecurity Framework.” https://www.nist.gov/cyberframework

New Jersey Cybersecurity and Communications Integration Cell. 2019. “Our Mission.” https://www.cyber.nj.gov/about

Newman, Lily. 2018. “The Ransomware that hobbled Atlanta will strike again” Wired.com. https://www.wired.com/story/atlanta-ransomware-samsam-will-strike-again/

Notification Required Following Breach of Security of Computerized Data. Texas Business and Commerce Code §521.053.

Obama, Barack. 2016. “Presidential Policy Directive PPD-41, United States Cyber Incident Coordination.”

Obama, Barack. 2013. “Presidential Policy Directive PPD-21, Critical Infrastructure Security and Resilience.”

Perry, Rick. 2004. “Executive Order by the Governor of the State of Texas RP32, Relating to Emergency Management and Homeland Security.”

Perry, Rick. 2005. “Executive Order by the Governor of the State of Texas RP40, Relating to the Designation of the National Incident Management System as the Incident Management System for the State of Texas.”

Perry, Rick. 2006. “Executive Order by the Governor of the State of Texas RP57, Relating to Implementing Recommendations from the Governor’s Task Force on Evacuation, Transportation, and Logistics.”

Pietri-Freeman, Roxette. 2019. “Louisiana school systems work to recover from cyber attacks.” KTBS.com. https://www.ktbs.com/news/louisiana-school-systems-work-to-recover-from-cyber-attacks/article_d93c736a-bfac-11e9-b690-b3d0930d9a6e.html

Prioritization. 6 U.S. Code §608.

Procedure for Declaration. 42 U.S. Code §5170.

Relating to the requirement that certain state and local government employees and state contractors complete a cybersecurity training program certified by the Department of Information Resources. Texas HR 3834, 86th Legislature.

Responsibilities of the Information Security Officer. Texas Administrative Code, §202.21.

Security Control Standards Catalog. Texas Administrative Code, §202.26.

Security Magazine. 2019. “Texas Passes Grid Protection Bills to Enhance Cybersecurity.” https://www.securitymagazine.com/articles/90267-texas-passes-grid-protection-bills-to-enhance-cybersecurity

Staff Responsibilities. Texas Administrative Code, §202.22.

State of Emergency. Texas Government Code, Chapter 433.

Sullivan, Emily. 2019. “Ransomware Cyberattacks Knock Baltimore's City Services Offline.” NPR. https://www.npr.org/2019/05/21/725118702/ransomware-cyberattacks-on-baltimore-put-city-services-offline

Texas Cybersecurity, Education, and Economic Development Council. 2012. “Report: Building a More Secure and Prosperous Texas.”

Texas Cybersecurity Act. TX HR 8, 85th Legislature.

Texas Division of Emergency Management. 2019a. “Executive Guide.” http://www.dps.texas.gov/dem/grantsresources/execguide.pdf

Texas Division of Emergency Management. 2019b. “Texas Emergency Management Executive Guide.” http://www.dps.texas.gov/dem/grantsresources/execguide.pdf

Texas Division of Emergency Management. Texas Administrative Code, Title 37, Chapter 7.

Texas Department of Information Resources. 2018. “Texas Cybersecurity Strategic Plan.” https://pubext.dir.texas.gov/portal/internal/resources/DocumentLibrary/Texas%20Cybersecurity%20Strategic%20Plan%202018.pdf

Texas Department of Information Resources. 2019. “Texas Cybersecurity Council.” https://dir.texas.gov/View-About-DIR/Information-Security/Pages/Content.aspx?id=133

Texas Interagency Coordination Center. 2019. “Texas Intrastate Fire Mutual Aid System (TIFMAS).” https://ticc.tamu.edu/Response/TIFMAS.htm

Texas Military Department. 2019. “Texas Military Department (TMD) Cyber Capabilities.”

Theophil, Morgan. 2019. “Jackson County fights to recover as computers remain under ransom.” Victoria Advocate.

Trump, Donald. 2017. “Executive Order 13800, Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure.”

U.S. Cybersecurity and Infrastructure Security Agency. 2019. “The National Cyber Incident Response Plan (NCIRP).” https://www.us-cert.gov/ncirp

U.S. Department of Homeland Security. 2006. “National Infrastructure Protection Plan Overview.” https://www.dhs.gov/xlibrary/assets/NIPP_Overview.pdf

U.S. Department of Homeland Security. 2013. “National Infrastructure Protection Plan 2013: Partnering for Critical Infrastructure Security and Resilience.” https://www.dhs.gov/sites/default/files/publications/national-infrastructure-protection-plan-2013-508.pdf

U.S. Department of Homeland Security. 2016a. “National Cyber Incident Response Plan.”

U.S. Department of Homeland Security. 2016b. “National Response Framework.” https://www.fema.gov/media-library-data/1466014682982-9bcf8245ba4c60c120aa915abe74e15d/National_Response_Framework3rd.pdf

Uria, Daniel. 2019. “Hack that cost Baltimore $18M a mystery after experts eye NSA link.” United Press International. https://www.upi.com/Top_News/US/2019/06/10/Hack-that-cost-Baltimore-18M-a-mystery-after-experts-eye-NSA-link/7961559775882/

AUTHOR BIOGRAPHIES

Dr. Danny W. Davis
Dr. Danny W. Davis is a retired Army lieutenant colonel. An infantryman, he spent much of his 20-year career with airborne, ranger, and special forces units. Upon leaving the service Danny worked overseas in a Department of State sponsored training program. He then spent six years in public education running a high school Junior ROTC program. He has also done consulting work for the US Army in the area of homeland security. With Texas A&M University's Bush School since 2010, Danny is an associate professor of the practice, his areas of interest are terrorism and cybersecurity policy. Danny holds two degrees from Texas A&M: a bachelor's in history and a Ph.D. in education. His master's in international relations was earned at Troy State University. He and his wife Mary live and raise cattle on the Lost Dog Ranch near Old Dime Box, Texas.

Amelia A. Boylan
Amelia A. Boylan is a second year at The Bush School of Government and Public Service at Texas A&M University where she is pursuing her Master of Public Service and Administration with a concentration in Security Policy and management. She is also working towards a Certificate in Homeland Security from the Bush School. She is a graduate of the United States Military Academy at West Point, where she majored in International Relations. She was commissioned as an U.S. Army Aviation Officer in 2010 and went to the U.S. Army's flight school at Ft. Rucker, AL where she learned to fly the AH-64 Apache helicopter. She deployed to Afghanistan in 2013 from Ft. Riley, KS. Amelia served as an Army Aviator until November of 2017. She currently lives in Houston, TX with her daughter and husband. BEAT NAVY!

Audrey N. Tepe
Audrey N. Tepe is a student and Graduate Research Assistant at the Bush School of Government and Public Service at Texas A&M University. She is studying for her Master of Public Service and Administration with a concentration in cybersecurity. She is also studying to obtain IT and cybersecurity certifications through CompTIA. Audrey holds a Bachelor of Science degree from Texas A&M University with a major in University Studies Leadership and double minors in psychology and sociology. She has interned with the Brazos County District Attorney's Office, Brazos County Sheriff's Office, and Texas A&M Cybersecurity Center. She is a Medical Accompaniment Volunteer and family advocate for her county's Child Advocacy Center.