Statement Before the United States Senate Committee on Homeland Security and Governmental Affairs

"What States, Locals, and the Business Community Should Know and Do: A Roadmap for Effective Cybersecurity."

Testimony of Amanda Crawford

Executive Director

Texas Department of Information Resources

February 11, 2020

Chairman Johnson, Ranking Member Peters, and members of the committee,

My name is Amanda Crawford, and I serve as the Executive Director for the Texas Department of information Resources ("DIR"). Thank you for inviting me to testify today. The mission of DIR is to serve Texas government by leading the state's technology strategy, protecting state technology infrastructure, and offering innovative and cost-effective solutions for all levels of government. We achieve this mission through a variety of ways including a robust Shared Technology Services – or managed IT-as-a-Service – program that allows entities at all levels of Texas government to focus their limited resources on mission rather than managing technology, and a multi-billion dollar cooperative contracts program that harnesses the buying power of the State of Texas to provide eligible government customers throughout the country with IT goods and services at aggressive discounts without a lengthy procurement process. DIR also sets the technology strategy for the State of Texas and, as you'll hear later in my testimony, plays a significant role in helping secure Texas from cyberattacks.

I would like to provide the committee with an overview of the August 2019 ransomware attack that impacted 23 local governments in Texas, focusing on the federal and state response and recommendations for the future. I will also discuss how Texas leverages cyber threat information from the Department of Homeland Security ("DHS") to protect its mission critical systems and assets. Finally, I will discuss the voluntary assistance provided by DHS-CISA to help Texas identify and address vulnerabilities, as well as avenues to make that assistance more robust.

State preparation and cooperation were the keys to the successful Texas response to the August 2019 Ransomware Incident.

As the State of Texas' technology agency, DIR is charged with many duties by statute. One of our primary missions, and the one I am here to speak with you about today, is cybersecurity. Our role in this space is two-fold. First, we serve as the internet service provider and network security operations center for many Texas state agencies. In that role, we detect and block malicious traffic over our networks. Second, the Office of the Chief Information Security Officer of Texas is a part of DIR. That office provides statewide information security program guidance to state agencies, institutions of higher education, and other governmental entities. Led by the

State of Texas Chief Information Security Officer, Nancy Rainosek, the team works to set state information security policies and standards, publish guidance on best practices, improve incident response preparedness, monitor and analyze incidents, coordinate security services, and promote information sharing throughout the public sector cybersecurity community. It was this second role, through the Office of the Chief Information Security Officer, that DIR was called into action to assist the 23 local government entities who were simultaneously attacked in the same ransomware event last August.

The attack began early in the morning on Friday, August 16, 2019. As public servants across the state came to work and discovered that their systems had been compromised and held hostage by ransomware, reports began filing into us at DIR. DIR was notified at 8:36 AM that eight local government entities across the state had been attacked. Over the next two hours, eleven more reports came in, and at approximately 10:30 AM it was reported that one of the impacted municipality's Supervisory Control and Data Acquisition ("SCADA") system had been rendered inoperable in the attack. This SCADA system controlled the monitoring and distribution of the entire local community's water supply. Given the number of entities impacted and the very real public health and safety threat, I notified the Office of the Governor to discuss the need to issue a disaster declaration.

Shortly after 11:00 AM, Governor Abbott issued the State of Texas' first statewide disaster declaration for a cyber event. With the Governor's disaster declaration, the Cybersecurity Annex to the Texas Emergency Management Plan was put into action. The disaster declaration also activated the Texas Division of Emergency Management's ("TDEM") State Operations Center ("SOC") to Level Two – meaning 24/7 operations. By noon, the SOC was fully active with state and federal incident responders reporting to the SOC. Leveraging the well-practiced logistics expertise of TDEM, Texas was able to have the first coordination call with all potentially impacted entities at 2:30 PM. Over the course of the incident, 23 impacted entities would be identified. The makeup of the victim pool was a representative sample of local governments across Texas.

By noon the following day, Saturday, August 17, 2019, Texas incident responders had identified and prioritized all impacted entities. By end of day Sunday, August 18, 2019, incident responders had made in-person visits to all impacted entities across Texas. And by the end of the day Friday, August

23, 2019 – one week after the incident began – all impacted entities had been remediated to the point that state support was no longer required.

While by no means perfect, the Texas response to this cyber event was a successful one. No ransom was paid in this event. While we are still collecting total costs to rebuild from the impacted entities, the current total cost for the state response is approximately one-tenth of the $2.5 million ransom demanded by the criminals responsible for this attack. The ability to bring these entities back online and into the rebuilding phase within one week can be attributed to extensive preparation and cooperation between the responders. In preparation for an event such as this, Texas took the following steps:

- **Senate Bill 64 (2019):** This legislation amended the definition of a disaster to include a cybersecurity event. Additionally, the bill allows the Governor to order the Texas National Guard to assist with defending Texas' cyber operations.
- **Cybersecurity Annex to the Texas State Emergency Management Plan**: In 2017, House Bill 8 called for DIR to create a statewide cybersecurity incident response plan. DIR coordinated the plan's development with the Texas Division of Emergency Management, the Texas Department of Public Safety, and the Texas Military Department. DIR held incident handling training and incident response exercises with response partners to ensure the ability to quickly operationalize the cybersecurity annex.
- **Managed Security Services Contract**: Through DIR's Shared Technology Services program, state and local governments can utilize a pre-negotiated cyber incident response contract with a managed security services vendor with no retainer fee. All contractors under this service are background-checked in advance so they are ready to assist on demand. Through the DIR contract, we have established competitive pricing as well as service level agreements for guaranteed response times and service quality and delivery.
- **State Operations Center**: Utilization of TDEM's State Operations Center was a key driver in our success. TDEM is prepared for communicating with the local entities through its district disaster coordinators and has critical tools to communicate with field teams. Additionally, local governments are accustomed to the communication channels from TDEM.

The other key to the Texas success in this event was the collaboration and cooperation of state and federal partners. Per the State of Texas Cybersecurity Annex, DIR led the incident response effort. Other state responders included:

- Texas Military Department (field incident response)
- Texas Division of Emergency Management (State Operations Center and logistics support)
- Texas A&M University System's Security Operations Center/Critical Incident Response Team (malware reversal, field support, and impact analysis)
- Texas Department of Public Safety (image capture)
- Public Utility Commission of Texas (consultative work)
- Texas Water Development Board (consultative work)
- Private sector vendors – both paid and volunteer – (field incident response)

Federal responders included:

- Federal Bureau of Investigation (criminal investigation)
- Department of Homeland Security (observation and malware reversal)
- Federal Emergency Management Agency (observation)

Texas greatly appreciates the participation of its federal partners in this event. The FBI teams worked well with the Texas responders and quickly assimilated with the other responders on this joint effort. They provided clear and timely information to us and were excellent partners on the forensic side of this mission. DHS-CISA also provided reverse engineering of the malware. However, early in the August event, there were miscommunications between DHS-CISA and state responders. These miscommunications primarily resulted from role confusion and a lack of clarity concerning what resources DHS-CISA could provide to help Texas. We have worked jointly to put plans in place to avoid the same missteps in the future. DHS-CISA has since initiated multiple meetings with DIR to address our concerns and propose solutions. Our communications with DHS-CISA have improved as a result of the August event.

Recommendations for improving federal participation include:

- **Better sharing of classified information with state government:** Currently, our receipt of timely and complete classified information about cyber threats facing our systems is sporadic.
- **Increasing DHS-CISA resources per region:** Having a dedicated resource to work with the Chief Information Security Officer of each state would help to drive incident response planning and preparedness and would better integrate federal resources into each state.
- **Clearly communicating what federal resources are available to state and local governments and how to receive those services:** Because these large-scale cyber incidents are a relatively recent development, clear delineations of roles and responsibilities have not been sufficiently communicated from the federal government to the state and local level. Multiple federal agencies provide cyber assistance of some sort and it can be challenging and inefficient, particularly in the middle of a cyber event, to know what help is available and who to call. A single federal point of contact who can then coordinate with other potential federal resources would be helpful.
- **Balancing the law enforcement need to protect investigations with the ability to share information about active threats:** It is critical to be able to share information with the cybersecurity community to prevent the same attack from occurring elsewhere. While we understand law enforcement's goal of catching the criminals responsible for these attacks, the ability to release more specific information would be helpful for the information security community who protects critical assets.

The interagency cooperation that occurred during this event is a testament to how government agencies at the federal, state, and local level can effectively work together to respond to critical events. No single agency could have responded successfully to the August ransomware incident. Absent these incident responders, the 23 local entities would have had great difficulty responding to the event without either paying the ransom or spending considerable time and resources trying to handle the situation on their own. While the August event was the first statewide cyber disaster declared in Texas, it will likely not be the last. We must prepare, as a state, for the next event, building and improving on our existing plan and anticipating what the next generation of cyber warfare will look like. Unfortunately, cyberattacks on state and local governments have become our new normal.

For example, DIR knows of 57 ransomware events that impacted state and local governments in Texas in 2019. This information comes from various sources including self-reporting, news articles, and partner notifications, as there is currently no statutory requirement for local government to report these events to DIR.

Organization Type	Number of Incidents
Cities	24
Counties	8
School Districts	15
Other Local Entities	6
State Agencies/Universities	4

Table 1: Ransomware Events Affecting Texas Governmental Entities in 2019

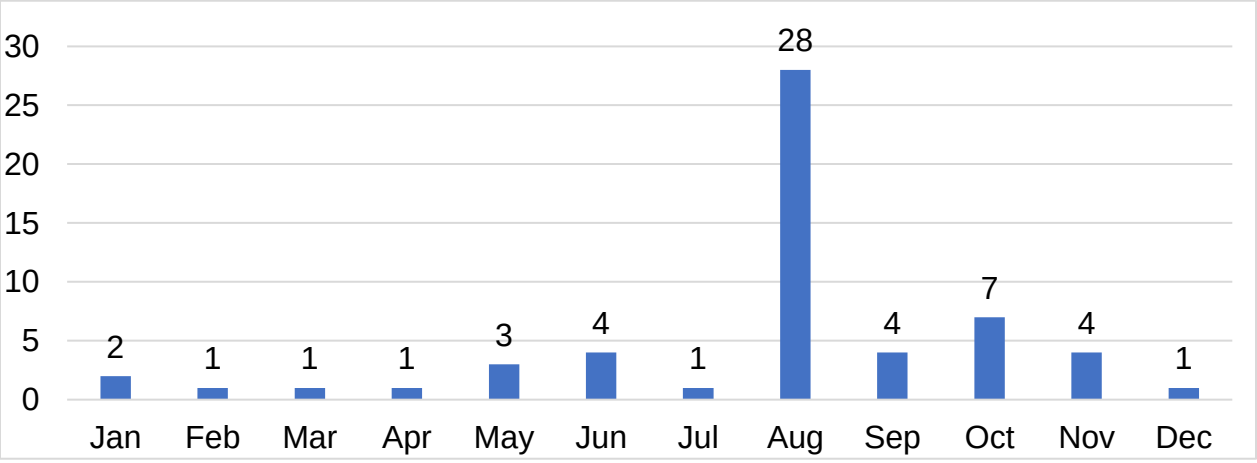

Chart 1: 2019 Texas Ransomware Incidents by Month

As Texas continues to face these events in 2020, MS-ISAC and DHS-CISA can be a valuable source for ransomware information, particularly at the local government level. Tracking trends and patterns can improve our education and outreach efforts and our ability to stop the next incident from occurring. Coordinated ransomware information sharing would be beneficial at both the state and national level.

Information received from DHS-CISA is one of the many valuable tools Texas uses to protect its critical assets and infrastructure. Additionally, DIR has a large Texas state and local government network for sharing information received from DHS-CISA.

Most of the federal information that Texas receives to improve the state's cybersecurity posture comes from the Multi-State Information Sharing and Analysis Center ("MS-ISAC"). This information consists of alerts from the Albert intrusion detection sensors and threat intelligence feeds with valuable indicators of compromise. Additionally, we benefit from their Vulnerability Management Program which provides website compromises, malware alerts, and notifications of compromised credentials.

The Albert sensors are a valuable addition to other intrusion detection capabilities at the state's Network Security Operations Center ("NSOC"), which is operated by DIR. These Albert sensors monitor inbound and outbound internet traffic and provide ransomware alerts to our NSOC. These alerts are actionable and have a low false-positive rate, which allows the DIR NSOC to take immediate steps to mitigate these cyber events.

The state also receives monthly reports from the MS-ISAC Vulnerability Management Program. This report notifies the state on outdated software that could pose a threat to state and local government systems. Using this report, DIR identifies and shares this information with our agency customers that own or maintain a vulnerable system. Because this is a comprehensive view of vulnerabilities across state and local entities in Texas, the report is voluminous and takes considerable time to review, assess, and then ultimately inform the potentially impacted entities. If this information could be shared in a more easily accessible format, it would enable states to send this information out to their vulnerable government entities more quickly.

Additionally, MS-ISAC is the state's main source of information regarding website defacements, particularly at the local government level. In fact, in

2020 alone, we have been informed of more than a dozen website defacements throughout Texas.

DIR also participates in pilot programs funded by DHS-CISA. Through these programs, Texas gains valuable information on strategies and new technologies to enhance the state's cybersecurity posture. For example, Texas is one of three states participating in a Johns Hopkins Security Orchestration and Automated Response ("SOAR") pilot funded by DHS-CISA. This will enable an automated update of indicators of compromise to decrease the time between discovery and mitigation of risk. Currently, DIR's NSOC cannot receive, and therefore cannot benefit from, automated updates from the Albert sensors because there are federally classified filters on these sensors. After the pilot is complete, if successful, Texas will still have to invest in orchestration tools at the state's expense.

DIR maintains a large mailing list of state and local government cybersecurity personnel to share all information received from various federal agencies, including DHS-CISA, MS-ISAC, and the FBI. We provide actionable and immediate alerts when necessary, and produce a weekly update consolidating other alerts. In addition, DIR hosts a monthly meeting during which we update the Texas cybersecurity community on significant issues and provide tabletop exercises, some of which are provided by MS-ISAC. Further, DIR is in the process of establishing the Texas Information Sharing and Analysis Organization for sharing threat and vulnerability information with both the public and private sector in Texas. This will tie together the federal and state information sharing efforts. Texas stands ready to share all timely and complete cybersecurity information that DHS-CISA can provide.

While the Department of Homeland Security offers many voluntary services, the wait times for receiving such services make them ineffective for securing Texas systems and critical assets.

DHS-CISA services that have been leveraged by Texas have been very valuable. Of note, the Texas Secretary of State had an election security assessment and penetration test provided by DHS-CISA which included testing of the State of Texas' consolidated data centers. That assessment provided good insight and actionable feedback on steps Texas could take to further improve the security posture of its systems. However, most of these voluntary services are not readily available for state and local governments.

If these services had more immediate availability, they could help state and local governments drive continuous improvement in cybersecurity. As it stands today, the wait times on some of these services can be a minimum of eighteen months. In cybersecurity, the entire threat landscape can change quite rapidly; and in technology eighteen months represents a full generation of change and advancement. Assessment and testing are only valuable if they are timely.

However, we are seeing improvements in communications and finding new ways to work with our DHS-CISA partners. One such novel engagement will occur in March at DIR's 20th annual Texas Information Security Forum ("ISF"), where over 400 state and local government security personnel gather to gain current cybersecurity education. This Forum is hosted by the State of Texas and free for any government security employee in the state to attend. DHS-CISA is working with DIR to provide an incident management workshop at the ISF. This workshop will consist of an overview of the process of detecting, analyzing, responding to disruptive events with the goal of mitigating the impact of a disruptive event and improving systems and processes to avoid future incidents.

As mentioned above, MS-ISAC is a valuable partner for Texas' cybersecurity program. They provide critical information sharing services and, when the partnership is working, it works well. Of course, no partnership is without room to improve. One area needing improvement is in event notification. Frequently, MS-ISAC will not inform the state when an incident has occurred at a local government entity somewhere in the state. This puts both the state and the local government entity at a significant disadvantage. In these cases, the state is unable to provide any assistance that would normally be available to the local government during their incident. Additionally, the states cannot collect data on attack trends or conduct pattern analysis to better protect state interests. States cannot respond if they are not notified.

In summary, DHS-CISA and the MS-ISAC provide valuable information and services to Texas when it comes to protecting its critical assets and information. While improvements can be made, we are engaged in continuing dialogue with both organizations to evolve the services and information we receive. Texas stands ready to assist in the continuing effort to enhance the security of our nation's assets and provide input when needed.

On behalf the state of Texas, I want to thank the Committee for addressing this important issue and inviting me to share our perspective with you. Thank you for your time and attention. I look forward to answering your questions.