Cybersecurity Incident Checklist

The cybersecurity incident response checklist details the inputs that will be necessary to establish a CONOP and determine what response resources may be necessary during an active cyber incident. Please complete the following sections to the best of your knowledge in consultation with your lead IT POC.

PRIMARY CONTACT INFORMATION (FIRST AND LAST NAME)	**CELL PHONE**	**WORK PHONE**	**HOME PHONE** (IF NO OTHER CONTACT AVAILABLE)	**EMAIL (IF AVAILABLE)**
TDEM District Coordinator Sarah Haak	214-629-4271	214-629-4271		Sarah.Haak@TDEM.Texas.gov
County/City/ISD/Entity IT POC (Individual Running Point)				
City/ISD/Entity Mayor/Managing Director				
City/ISD/Entity EMC				
City/ISD/Entity Police Chief				
City/ISD/Entity Fire Chief				
County Judge				
County EMC				
County Sheriff				
County Fire Marshall				
DIR	24/7 HOTLINE: 877-347-2476			
DPS Regional Intel/Fusion Center				
FBI	FBI Field Office Dallas - Cyber: Supervisor (Ransomware) Richard Murray – 972-559-5231 RJMurray@fbi.gov	FBI Field Office Dallas - Cyber: Field Agent (Ransomware) Joshua Jacobs – 817-905-6191	FBI Field Office Dallas - Cyber: Supervisor (XXXX) Brett Leatherman – 972-559-5132 BELeatherman@fbi.gov	
US Secret Service				
DHS				

EOC Activated (Yes/No)

EOC Designation (name):

□ Level 1 (Emergency Conditions/Full Activation)

□ Level II (Escalated Response Conditions/Partial Activation)

□ Level III (Increased Readiness Conditions/Monitoring)

□ Level IV (Normal Operations/Steady State)

EOC location (Full address):

EOC Contact Number:

Notes:

Situation Timeline

Date incident occurred/detected:

Breach type (if known):

Date of the last vulnerability scan (If Known):

Immediate action taken:

Entities/Departments impacted (List As Many As Possible):

Does the ISD/City/County/Impacted Entity have Cybersecurity insurance (Yes/No/Unknown):

If YES, What kind of Cybersecurity insurance is carried (Privacy/Full Coverage):

If YES, has the insurance company been contacted? (Yes/No/Unknown):

Is a Photo of the ransom note available to be shared with investigating parties (Yes/No/Unknown):

Any other relevant details to share:

INCIDENT REPORTING/NOTIFICATIONS:

□ Law Enforcement:

  □ ISD Police Department

  □ City Police Department

  □ County Sheriffs Office

  □ DPS

  □ FBI

  □ Secret Service

□ MSISAC

□ Other

□ DDC/DC

□ SOC

□ DIR

□ TEA (For ISD's and Educational Institutions)

□ TDCJ (For Jails and Prisons)

□ DSHS (For entities whose patient records are impacted)

**NOTE: The DPS Regional Intel Contact can help a jurisdiction verify if any other entities have been impacted. They can assist with running an inquiry through the fusion center.

RESPONDING AGENCIES/DEPARTMENTS (Please list all that are currently involved in the active response):

Information Technology Support Overview Information:

☐ IT handled internally to the ISD/City/County/Entity

☐ ISD/City/County/Entity uses a Managed Service Provider (MSP)

IF MSP Provide Contact Information:

Company Name:
Contact Name:
Cell Phone:
Email:

☐ How many ONSITE IT personnel are supporting the ISD/City/County/Entity? (Provide a total number physically located at the site)

Number of personnel:

Location of personnel:

Situation Impacts/ Critical Infrastructure

Departments Impacted:

☐ How many County/City/ISD/Entity departments were impacted? (Total #)

☐ Which County/City/ISD/Entity departments were infected? (List all)

SCADA Systems:

☐ Water systems impacted?

☐ Legal video surveillance requirements? (eg. Pump/lift stations)

☐ Electrical systems impacted?

☐ Traffic management systems impacted?

Police Department Systems:

☐ Impacts to TLETS access? (Yes or No)

- ☐ Do you have the TLETS back up instructions? (Yes or No)
    - ☐ See attached TLETS back up instructions

☐ 911 system impacted? (Yes or No)

- ☐ Do you have a backup PSAP? (Yes or No)

☐ Dispatch capabilities? (Yes or No)

☐ Impacts to Records Management? (Yes or No)

- ☐ Have you made contact to the OAG? (Yes or No)
- ☐ Have you notified open records 877-OPEN-TEX for guidance? (Yes or No)

☐ Impacts to incar/body worn cameras? (Yes or No)

- ☐ How long until the hard drives are full and video can no longer be stored/captured?
- ☐ Do you still have access to previous video storage? (Yes or No)

City/County Jail Systems:

☐ Physical Security system impacts? (Yes or No)

☐ Detainee records management system impacts? (Yes or No)

☐ Has notification been made to TDCJ or surrounding facilities incase transfers become necessary? (Yes or No)

Fire Department Systems:

☐ 911 system impacted? (Yes or No)

- ☐ Do you have a backup PSAP? (Yes or No)

☐ Dispatch capabilities? (Yes or No)

☐ Impacts to Records Management? (Yes or No)

- ☐ Have you made contact with DSHS for reporting requirements? (Yes or No)
- ☐ Patient records/data impacts? (Yes or No and List impacts)

ISD Systems:

☐ Is the impacted ISD in session? (Yes or No)

☐ Do they have good backups or are those backups encrypted?

Financial Management Systems:

☐ Accounts receivable system impacts? (Yes or No)

☐ Accounts payable system impacts? (Yes or No)

- □ Is employee payroll impacted? (Yes or No)
- □ Date of next scheduled payroll submission:

□ Are you able to purchase/spend county/city/isd/entity funds? (Yes or No)

Additional Critical Infrastructure Impacts:

□ Citizen information compromised? (Yes or No)

□ Additional Information/Impacts?

RESORATION PRIORITIES:

What are the most important systems to restore first?

What order should the most critical departments be restored in?

IT Infrastructure/Hardware Impacts

Brand Impacted:

□ Apple

□ Dell

□ Lenovo

□ Asus

□ Acer

□ Microsoft

□ Toshiba

□ Samsung

□ HP

□ Sony

□ MSi

□ IBM

□ Intel

□ Other

Firewalls:

□ What firewall/s does your City use? (Yes/No/Unknown)

Operating Systems:

□ Windows 7

□ Windows 10

□ Other:

Total Number of Devices:

□ Desktop/Laptops:

□ Servers:

☐ Phones:

☐ Networks:

☐ Additional Hardware:

Confirmed infections:

☐ How many systems were confirmed to be infected? Note that some may have been taken off line to protect or because you weren't sure, how man were actually confirmed? (Total Number):

Physical sites impacted:

☐ Total number of physical sites or locations effected?

☐ How far apart are the sites?

Back Up Systems impacted:

☐ What backup systems does the City/County/ISD/Entity utilize?

☐ Does the City/County/ISD/Entity utilize onsite storage?

- ☐ Has it been compromised? (Yes or No)
- ☐ Last Back Up Date?

☐ Does the City/County/ISD/Entity utilize offsite backup storage?

- ☐ Has it been compromised? (Yes or No)
- ☐ Last Back Up Date?
- ☐ Is it a complete back up or just an image of the databases with no programs?

Other Information:

Public Information

☐ Is the City/County/ISD/Entity PIO engaged? (Yes/No/Unknown)

☐ Has a public release been issued? (Yes/No/Unknown)

- ☐ Systems used for public information compromised? (Yes/No/Unknown)

☐ Media contact information compromised? (Yes/No/Unknown)

☐ Do you still have access to your contact lists? (Yes/No/Unknown)

☐ PIO support needed? (Yes/No)

☐ Have you linked to any of the following:

- ☐ DIR PIO (Yes/No)
- ☐ NCTCOG NXTPIO Group (Yes/No)
- ☐ DPS PIO (Yes/No)

☐ Is a JIC necessary? (Yes/No)

Resource Request Considerations

☐ Best staging or deployment physical location for and resources deployed? (Provide physical address):

STAR Requests:

☐ Does Jurisdiction have access to WebEOC to submit STARs? (Yes/No/Unknown)

☐ Requested a fusioned incident in WebEOC: (Yes/No)

Disaster Declaration:

☐ Is the jurisdiction considering a Disaster Declaration? (Yes/No)

Notes to assist in that determination:

☐ Disaster Dec needed to deploy state response team led by DIR.

☐ DIR will offer AT&T response team as first solution at the jurisdictions expense (~$20,000) without a disaster declaration.

☐ DIR assistance beyond that is consulting in nature.

☐ Procurement considerations – 30 days to 7 days for bidding out contracts

☐ Documenting their bad day – future grant implication

State IT Response Resources Available:

☐ AT&T Cyber Team (contract county/city has to pay for)

☐ DIR

☐ TMD Cyber teams

☐ TAMUS Cyber Team

Internal Communication/Confidentiality Considerations

☐ NOTE: Preface all communication with "Confidential". Information should be shared only with those who have a legitimate need to know

☐ ****CONFIDENTIAL: Do Not Disseminate Beyond Original Distribution****

☐ Be prepared for non-impacted jurisdictions to call requesting information. Think through your CAN response ahead of time. This will all be part of an ongoing criminal investigation, you are not at liberty to share any details.

Next Steps and Additional Considerations

The following section provides details and insight on the next steps once the situation size up is complete. It includes notes from lessons learned during previous cybersecurity incidents on how a city/county/ISD/Entity can get ready for the initial site visit with a team deployed to assist (regardless if they are from an insurance company or government resources, recovery notes and best practices to reinforce.

Getting Ready for a Site Visit

Phase	Questions
Site Visit Team Make Up	▪ If a State team is deployed members could include personnel from TMD, DPS, FBI, DIR vendor AT&T, Core Recon, TAMUS Cyber Team
Site Visit Preparation	▪ Need a POC from every jurisdiction with home/cell contact phone numbers. ▪ Need an established meeting location with POC. ▪ Make sure access to all impacted locations are available for the site visit team. ▪ City/County/ISD/Entity Coordination – ▪ Visit with personnel in your other departments to understand total scope. ▪ To ensure total situation is assessed, do not demob the site visit team to leave until each impacted department meets with them. ▪ **What are the most important systems you need back on line first?**
Scope of Visits	▪ Site Visits are **meant** to assist with the discovery and assessment phase. ▪ Team will work to determine what systems are down ▪ What are the extent of the impacts? ▪ Cause and impacts on your entity? ▪ Some of this site visit will be focused on investigation and response to collect information to investigate the attack. ▪ Goal ultimately is to assess the best forth forward. ▪ Documenting their bad day – future grant implications
After Site Visit Expectations	▪ Site team visits will work with DDC/SOC and entities to help build a best path forward to recover ▪ Resources available towards recovery: ▪ Discovery, triage, and assessment services ▪ Cities are responsible for recovery actions ▪ There are many vendors who provide these services in the private sector. ▪ This is the fastest path to recovery. ▪ Entity can go through city or county to procure ▪ Entity can use cooperative process through DIR contracts to procure recovery services

	▪ Most important focus is logistics so that we can coordinate assistance. Coordination is a critical function of this next phase.

Recovery Notes

Phase	Questions
Contracting and Purchasing Information for Impacted Entities	▪ The Texas Department of Information Resources (DIR) leverages the state's purchasing power to negotiate competitive discounts on information and communications technology products and services. DIR's streamlined cooperative purchasing program allows Texas public entities to purchase through pre-negotiated contracts that meet stringent state procurement requirements. Every dollar that participants save on the purchase of goods and services through this program is a dollar that can be redirected to agencies' mission-critical services. ▪ The following contract types offer various networking products and services for purchase or seat management services. The management services contracts can help you rebuild your networks or systems to ensure your systems are up-to-date and able to function in today's technology environment. In addition, to assist public entities in their recovery efforts, DIR has negotiated the addition of network components to the Dell Bulk Purchase Initiative, including servers, other networking hardware, and network virtualization products.
Option 1: Dell Bulk Purchase Initiative	▪ Dell is fully committed to assisting DIR and the affected public entities by providing additional discounts on enterprise infrastructure through the Dell Bulk Purchase Initiative. As the requirements and configurations are likely to vary significantly from one entity to the next, the discount grid located here are minimum discounts. As specific requirements lead to specific configuration requests, additional discounts may be applied.
Option 2: Network Products and Related Services Contracts	▪ These contracts offer data storage, data communication & networking products and related services. Customers can purchase directly through this DIR contract. Contracts may be used by state and local government, public education, other public entities in Texas, as well as public entities outside the state.
Option 3: Managed Services End-User IT	▪ These contracts offer end-user IT outsourcing (managed services) for information technology assets. Managed services include hardware provisioning and desktop services, asset tracking and many other services. Contracts may be used by state and local government, public education, other public entities in Texas, as well as public entities outside the state.
Option 4: Information Technology	▪ These contracts offer ITS products and services that provide the means to maintain the confidentiality, integrity, and accessibility of data, computing systems, networks and IT environments. Customers can purchase directly through

Security (ITS) Products and Services	these DIR contracts. Contracts may be used by state and local government, public education, other public entities in Texas, as well as public entities outside the state.
DIR Contact Information	▪ For assistance using DIR's Cooperative Contracts, please contact: ▪ Kelly Parker, CTCM, CTPM ▪ Director, Cooperative Contracts ▪ Kelly.Parker@dir.texas.gov | o: 512.475.1647
Notes	▪ Confirmed that local governments can utilize DIR contracts without any membership requirements or restrictions, i.e., they do not have to be a member of the CPA/SPD cooperative purchasing program. ▪ The contract is DIR-TSO-3820, AT&T Corp. AT&T has various contracts with DIR for various types of services. There are also subcontractors available on this specific contract. (https://dir.texas.gov/View-Search/Contracts-Detail.aspx?contractnumber=DIR-TSO-3820&keyword=DIR-TSO-3820)
Additional Information	▪ Link for larger list of DIR contracts with various cyber-type services to include rebuilding (https://dir.texas.gov/View-Search/Contracts.aspx?keyword=cyber) ▪ Link to the purchasing initiatives that the impacted entities might find helpful: https://dir.texas.gov/View-About-DIR/Article-Detail.aspx?id=209

Best Practices to Reinforce

Phase	Questions
Best Practices	▪ Push available mitigation efforts to IT departments and users (password, security software updates, ect). ▪ Patching efforts can protect entities in general from most bugs out there currently ▪ Do not delete encrypted data as once it is deleted you will never be able to get them back if a decryption key is found in the future.

TLETS Agency Fall Back

Texas Law Enforcement Agencies (LEA) are currently experiencing an increase in malware attacks, some of which have resulted in the successful installation of ransomware. In the event of a compromise, it is critical to disconnect any impacted system(s) immediately, as containment is key. Disconnected LEAs are still obligated by statute to report certain information to state systems.

Phase	Questions
Entry Requirements	1) Missing Person entry (Chapter 63 Code of Criminal Procedure) 2) Protection Order entry (Chapter 86 Family Code) 3) Wanted person entry (Chapter 2.195 Code of Criminal Procedure) 4) Threats Against Peace Officers entry (Chapter 411.048 Texas Government Code) 5) Criminal History (Chapter 66 Code of Criminal Procedure) 6) Gang information (Chapter 67 Code of Criminal Procedure) 7) Sex Offender registration and verification (Chapter 62 Code of Criminal Procedure)
Notes	Entry types 1-4 are NCIC/TCIC files for which entry must be accomplished through a TLETS connection. While Entry types 5-7 be done electronically, reporting via paper or on portable media is acceptable while an entity is in a disconnected state.
Solutions for LEA’s Disconnected from TLETS	▪ Hosted entry ▪ A LEA may request that a different LEA enter records on their behalf. DPS suggests that the host agency seek to be authorized to enter utilizing the ORI of the impacted agency so that when normal service is restored, there would be no need to reenter the record with the owning agency ORI. ▪ Hosted Query ▪ A LEA may request that a different LEA query records on their behalf via TLETS. ▪ Traffic Rerouting ▪ One LEA’s traffic can be routed to another agency. This will allow for hit confirmations to occur if the hosting agency can access the supporting documentation for the warrants from the rerouted LEA via their electronic records management system (ERMS) or hard copy access.
Notes	▪ To facilitate these TLETS related solutions, disconnected LEAs must ask another LEA to serve as a host during the time the LEA is disconnected. Once a host LEA has been identified, the DPS Operations Information Center (OIC) can reroute TLETS traffic to the host agency and also authorize the host agency to use the ORI of the disconnected LEA.
OIC Contact Information	▪ DPS Operations Information Center ▪ OIC@dps.texas.gov ▪ 1-512-424-2139

Authority

Strategic planning guidance and authorities governing the enactment and implementation of this cyber incident guide are summarized below.

The following table presents specific sources, their relevance to this document, and hyperlinks to their online location.

Source	Relevance	Link
Texas Government Code **Chapter 418**	Provides authority and mechanisms to clarify and strengthen key roles, as well as authorize and provide for cooperation and coordination of an emergency management system embodying all aspects of predisaster preparedness and postdisaster response.	http://www.statutes.legis.state.tx.us/Docs/GV/htm/GV.418.htm
Texas Government Code **Section 418.050**	Provides guidelines for reentry of areas previously evacuated because of a disaster or threat of disaster.	http://www.statutes.legis.state.tx.us/Docs/GV/htm/GV.418.htm#418.050
Texas Government Code **Section 418.11**	Describes the Texas Statewide Mutual Aid System.	http://www.statutes.legis.state.tx.us/Docs/GV/htm/GV.418.htm#418.018
Executive Order (EO) 13636	Improving Critical Infrastructure Cybersecurity	
National Institute of Standards and Technology (NIST) Cybersecurity Framework	NIST provides public and private entities with cybersecurity standards, guidelines, and best practices.]	
Presidential Policy Directive 21 (PPD-21)	National Infrastructure Protection Plan (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.	
Presidential Policy Directive 41 (PPD-41)	Directed the establishment of a National Cyber Incident Response Plan (NCIRP	
The Robert T. Stafford Disaster Relief and Emergency Assistance Act (Stafford Act)		

Texas Government Code Chapter 2054	
Texas Government Code Chapter 421	
Texas Government Code Chapter 433	
Texas Administrative Code, Part 10 DIR, Chapter 202	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."
Texas House Bill (HB) 8 - Texas Cybersecurity Act	Established an Information Sharing and Analysis Center (ISAC) ISAC is anchored in Texas Government Code §2054.0594.
Texas House Bill (HB) 9 - Texas Cybercrime Act	"Updates the Texas Penal Code to recognize several new types of cybercrime and their punishments."

For More Information

For more information on this field operations guide contact Sarah Haak, District Coordinator, at Sarah.Haak@tdem.texas.gov.

Produced by the Texas Division of Emergency Management
Field Response Section, Region 1, DDC 4B Garland
www.tdem.texas.gov