Texas Volunteer Incident Response Team

Program Handbook

December 1, 2021

Table of Contents

Purpose

Texas Government Code Section 2054.52002 directs the Texas Department of Information Resources (DIR) to establish the Texas Volunteer Incident Response Team (VIRT) and provide eligible public entities rapid cybersecurity incident response assistance. Many government organizations do not have the budget or resources to employ onsite staff with the expertise to respond appropriately after a cyberattack. The goal of the VIRT is to provide those government organizations with support so that the services those organizations provide to Texans are not disrupted.

The Texas VIRT is comprised of volunteers with expertise addressing cybersecurity events that quickly respond to significant cybersecurity incidents and provide support to eligible participating entities, including Texas agencies, institutions of higher education, and local government organizations. Volunteers provide support to participating entities in concert with DIR and other state level response resources.

The Texas VIRT Program Manual provides guidelines for the VIRT's operation. Additionally, Texas Government Code defines key terms relevant to the VIRT. These definitions are provided in the table below.

Term	Definition
Incident Response Team	Texas volunteer incident response team established under Texas Government Code Section 2054.52002.
Participating Entity	A state agency, including an institution of higher education, or a local government that receives incident response team assistance during a cybersecurity event.
Volunteer	An individual who provides rapid response assistance during a cybersecurity event, as part of the Incident Response Team.

VIRT Program Background

As per Texas Government Code Section 2054, Subchapter N-2:

- DIR prescribes eligibility criteria for participation as a volunteer on the incident response team and has sole discretion to determine whether an individual is qualified to serve as a volunteer.
- DIR will enter into a contract with eligible VIRT volunteers.
- Volunteers consent to a background screening during the application process and may be subject to ongoing or routine monitoring.
- Volunteers will acknowledge the confidentiality of incident information and protect it from unauthorized disclosure.
- Volunteers are responsible for avoiding conflicts of interest that might arise during an incident response team deployment.
- Volunteers deployed to support incident response activity act in concert and with the consent of DIR and report activities and status back to DIR.
- A volunteer is not an agent, employee, or independent contractor of the state, and the state is not liable for personal injury or property damage sustained by the volunteer from participation in the incident response team.

- A volunteer who in good faith provides professional services in response to a cybersecurity event is not liable for civil damages because of the volunteer's acts or omissions, while serving on an authorized VIRT deployment.
- A volunteer may receive reimbursement for actual and necessary travel and living expenses incurred while on an authorized VIRT deployment.

VIRT Overview

VIRT Mission Statement

The Texas Volunteer Incident Response Team lends support to impacted Texas entities in response to critical cybersecurity events.

VIRT Deployment Scenario

The scenario below provides an example of when the Texas VIRT could be deployed.

> Threat actors, using a new ransomware-as-a-service platform, have successfully exploited a large managed service provider, who has over 1,000 customers across the state of Texas. Many of these customers have been impacted by this ransomware variant and are unable to access even their basic IT systems.
>
> In response to this threat, the Texas Governor has issued a disaster declaration for the impacted jurisdictions and activated the Texas State Operations Center to Level II – Enhanced Response Conditions. DIR has requested the support of state resources, but additional incident response personnel are needed. In response to the disaster declaration and requests for assistance from multiple participating entities, the Texas Volunteer Incident Response Team (VIRT) has been activated to quickly support the impacted jurisdictions with incident response activities.

Members of the VIRT would have the opportunity to support those impacted entities as they progress through the initial phases of incident response.

VIRT Activation Requirements

If a major cybersecurity event occurs in Texas, the Texas VIRT provides a method for individuals with the necessary skills and expertise in cybersecurity incident response to support statewide incident management efforts and provide rapid assistance to requesting participating entities.

DIR may deploy VIRT volunteers given the following criteria:

- The governor declares a state of disaster caused by a cybersecurity event; or,
- A cybersecurity event occurs and affects multiple participating entities.

VIRT Volunteers

VIRT volunteers will use their skills and expertise to serve the state during a cybersecurity disaster.

Volunteer Eligibility

VIRT volunteers must meet the following eligibility criteria:

- Expertise in addressing cybersecurity events including knowledge, skills, and abilities in cybersecurity incident response.
- Ability to successfully complete a background check, which is subject to periodic reverification.
- Agree to sign a contract with DIR, which outlines:
    - Volunteer information confidentiality and non-disclosure;
    - Requirements to avoid conflicts of interest during a deployment; and
    - Other specifications relevant to the operation of the VIRT.
- Ability to travel to an incident site or operations center on short notice for a defined period of time or to provide remote support, as appropriate.

Volunteer Application Process

A prospective volunteer should review the Texas VIRT Program Manual, and if eligible, complete and submit the Texas VIRT Volunteer Application.

Application Overview

The Texas VIRT Volunteer Application gathers the following information:

- Personal contact information
- Education and background
- Application narrative, including:
    - Two narrative responses
    - Professional references
- Knowledge, skills, and abilities
- Attestation to membership requirements and considerations
- Application signature
- Privacy considerations

Submission and Review Process

Each application will be reviewed by DIR staff according to a defined process, summarized below.

- VIRT applicant will complete and submit a VIRT volunteer application.
- DIR will provide VIRT applicant with a confirmation of application receipt.
- DIR staff will review the completed application, using the following criteria:
    - Application is complete and signed.
    - Application exhibits expertise in addressing cybersecurity events.
        - Expertise is gathered from the application's narrative, education and background, and knowledge, skills, and abilities sections.
        - The review is performed in line with the criteria defined in Appendix A – VIRT Volunteer Abilities, Knowledge, Skills, and Tasks.
    - VIRT applicant consents to the membership requirements and administrative considerations.
    - Validation of application content based on discussion with provided references and any other methods DIR deems appropriate.
- If the application is accepted, the VIRT applicant will be notified via email.
- A VIRT applicant whose application is accepted will be sent instructions from DIR Human Resources to complete a FAST fingerprint-based criminal history check.
- DIR will securely receive and review the results of the criminal history check.
    - DIR Human Resources staff will provide a recommendation as to the disposition of the VIRT applicant's eligibility for membership and notify the applicant of the results.
    - VIRT applicants who fail the background check will be notified of the results.
        - The applicant shall be afforded the opportunity to prove that they are not the subject of the criminal history information or to correct incorrect information in the criminal history record with the appropriate law enforcement agency.
- A VIRT applicant who pass the background check will be sent the Department of Information Resources Volunteer Contract and Non-Disclosure Agreement for the Texas Volunteer Incident Response Team, via email, for signature.
- After the signed volunteer contract is received by DIR, the volunteer will be officially notified via email of final acceptance of VIRT membership and will complete additional onboarding paperwork.

If a VIRT applicant has a question or issue during the application process, they can email TexasVIRT@dir.texas.gov.

VIRT Participating Entity

As authorized by Texas Government Code Section 2054.52005, on the request of a participating entity, the Texas VIRT incident response team may respond to a cybersecurity event that affects multiple participating entities or is in response to a Governor's disaster declaration to a cybersecurity event.

Eligible Organizations

Texas Government Code Section 2054.52001 defines "participating entities" as "a state agency, including an institution of higher education, or a local government" that receives assistance from the VIRT during a cybersecurity event. These entities include:

- State agencies
- Institutions of higher education
- Public junior colleges
- Cities
- Counties
- School districts
- Special districts or other political subdivisions of the state

Support Requirements

In order to receive cybersecurity support from the Texas VIRT, an entity must be eligible to participate under Texas Government Code Section 2054.52001 and must request assistance from DIR.

Requesting VIRT Assistance

Eligible organizations impacted by a cybersecurity event may request incident response support from Texas DIR by calling DIR's 24/7 security hotline at 877-DIR-CISO (877) 347-2476.

During initial discussions between DIR and the impacted entity, the entity may request VIRT volunteer support.

During this discussion, specific needs and technological skillsets may be identified to provide the appropriate VIRT resources in support of the incident response activities. VIRT resources will be provided based one incident complexity, resource availability, and available skillsets.

Participating Entity Agreements

When the complexity of the event and the urgency of providing incident response services necessitate or allow, DIR may require the participating entity to sign a Memorandum of Understanding prior to obtaining assistance from the incident response team.

Participating Entity Issues Management

Should a participating entity experience an issue with any member of the Texas VIRT incident response team, the entity should call DIR's 24/7 security hotline at (877) 347-2476 and ask to speak to the Texas VIRT Coordinator.

The coordinator will quickly investigate and address any issues that arise to ensure continued professional incident response support is provided to the participating entity.

Document Version History

Version	Date	Comments
1.0	December 1, 2021	Initial Publication

Appendix A – VIRT Volunteer Abilities, Knowledge, Skills, and Tasks

The following skillsets and knowledge areas will be considered as part of the VIRT volunteer application evaluation process.

These functions align with the National Initiative for Cybersecurity Careers and Studies (NICCS) Cyber Defense Incident Responder and other relevant roles.

Abilities

Volunteers on the Texas VIRT should have some of the following abilities:

- Ability to apply critical reading/thinking skills and think critically to solve problems.
- Ability to communicate calmly, clearly, and professionally with a varied group of stakeholders including elected officials and executive leadership.
- Ability to prioritize and allocate cybersecurity resources correctly and efficiently.
- Ability to tailor technical and planning information to a customer's level of understanding.
- Ability to understand concepts and issues related to cybersecurity and its organizational impact.
- Ability to understand technology, management, and leadership issues related to organization processes and problem solving.
- Ability to relate strategy, business, and technology in the context of organizational dynamics.

Knowledge

Volunteers on the Texas VIRT should have knowledge in some of the following areas:

- Knowledge of incident categories, incident responses, and timelines for responses.
- Knowledge of incident response and handling methodologies.
- Knowledge of computer networking concepts and protocols, and network security methodologies.
- Knowledge of risk management processes (e.g., methods for assessing and mitigating risk).
- Knowledge of laws, regulations, policies, and ethics as they relate to cybersecurity and privacy.
- Knowledge of cybersecurity threats and vulnerabilities.
- Knowledge of specific operational impacts of cybersecurity lapses.
- Knowledge of data backup and recovery.
- Knowledge of business continuity and disaster recovery continuity of operations plans.
- Knowledge of host/network access control mechanisms (e.g., access control list, capabilities list).
- Knowledge of network services and protocols interactions that provide network communications.
- Knowledge of intrusion detection methodologies and techniques for detecting host and network-based intrusions.
- Knowledge of network traffic analysis methods.

- Knowledge of what constitutes a network attack and a network attack's relationship to both threats and vulnerabilities.
- Knowledge of cybersecurity defense and information security policies, procedures, and regulations.
- Knowledge of cybersecurity attackers (e.g., script kiddies, insider threat, non-nation state sponsored, and nation state sponsored).
- Knowledge of system administration, network, and operating system hardening techniques.
- Knowledge of cyber-attack stages (e.g., reconnaissance, scanning, enumeration, gaining access, escalation of privileges, maintaining access, network exploitation, covering tracks).
- Knowledge of network security architecture concepts including topology, protocols, components, and principles (e.g., application of defense-in-depth).
- Knowledge of malware analysis concepts and methodologies.
- Knowledge of an organization's information classification program and procedures for information compromise.
- Knowledge of network protocols such as TCP/IP, Dynamic Host Configuration, Domain Name System (DNS), and directory services.
- Knowledge of the common networking and routing protocols (e.g. TCP/IP), services (e.g., web, mail, DNS), and how they interact to provide network communications.

Skills

Volunteers on the Texas VIRT should have skills in some of the following areas:

- Skill of identifying, capturing, containing, and reporting malware.
- Skill in preserving evidence integrity according to standard operating procedures or national standards.
- Skill in securing network communications.
- Skill in recognizing and categorizing types of vulnerabilities and associated attacks.
- Skill in performing damage assessments.
- Skill in using security event correlation tools.

Tasks

Volunteers on the Texas VIRT should have proficiency performing some of the following tasks:

- Coordinating incident response functions.
- Performing cybersecurity defense incident triage, to include: determining scope, urgency, and potential impact; identifying the specific vulnerability; and, making recommendations that enable expeditious remediation.
- Performing initial, forensically sound collection of images and inspecting to discern possible mitigation/remediation for enterprise systems.
- Coordinating and providing expert technical support to assist enterprise-wide cybersecurity defense technicians in resolving cybersecurity defense incidents.
- Correlating incident data to identify specific vulnerabilities and make recommendations that enable expeditious remediation.

- Analyzing log files from a variety of sources (e.g., individual host logs; network traffic logs; firewall logs; and intrusion detection system [IDS] logs) to identify possible threats to network security.
- Performing cybersecurity defense trend analysis and reporting.
- Performing real-time cybersecurity defense incident handling (e.g., forensic collections; intrusion correlation and tracking; threat analysis; and direct system remediation) tasks to support deployable Incident Response Teams (IRTs).
- Receiving and analyzing network alerts from various sources within the enterprise and determining possible causes of such alerts.
- Tracking and monitoring cybersecurity defense incidents from initial detection through final resolution.
- Serving as technical expert and liaison to law enforcement personnel and explaining incident details, as required.
- Coordinating with intelligence analysts to correlate threat assessment data.
- Writing and publishing after-action reviews.

Appendix B – Texas VIRT Documents

The table below provides links to the relevant documents that support the operation of the Texas Volunteer Incident Response Team.

Document	Permanent Link
Texas VIRT Volunteer Application	On DIR Website: https://dir.texas.gov/information-security/cybersecurity-incident-management-and-reporting
Texas VIRT Volunteer Contract/NDA Sample	On DIR Website: https://dir.texas.gov/information-security/cybersecurity-incident-management-and-reporting
Texas VIRT Participating Entity Memorandum of Understanding Sample	On DIR Website: https://dir.texas.gov/information-security/cybersecurity-incident-management-and-reporting