2020 Biennial Performance Report
Consolidated Network Security System

This report addresses Government Code, Section 2059.057, which requires the Texas Department of Information Resources (DIR) to describe the consolidated network security system's accomplishment of service objectives and other performance measures, including financial performance.

Background

Cybersecurity is about protecting the confidentiality, integrity, and availability of data. It also includes securing the associated information resources that transmit or store that data. It is an ongoing process that requires continuous, coordinated, and focused effort by all state agencies. DIR, in consultation with agencies, continues to develop and expand its ability to monitor, assess, and assist in the safeguarding the state's information infrastructure from cyber-attacks.

DIR manages a statewide information security program, which coordinates with agencies to protect state information and elevate the security posture and capabilities of the state. DIR's Office of the Chief Information Security Officer (OCISO) oversees the statewide information security program which includes:

- cybersecurity governance, policy, and planning,
- comprehensive security program risk assessments,
- technical security assessments including mobile, web application, and network penetration testing,
- security education and training, and
- a statewide portal for agencies and institutions of higher education to track incidents, assess security risks, monitor policy compliance, and report on their status according to the Texas Cybersecurity Framework.

DIR also manages the Network and Security Operations Center (NSOC), a secure and resilient facility hosting both security and network operations. The NSOC is tasked by the state legislature with providing perimeter network security for the State of Texas networks and agencies. The NSOC also supports the statewide information security program and works closely with the OCISO to provide a more secure computing environment for the State of Texas through:

- security event monitoring and analysis, alerts, and incident response coordination,
- network intrusion detection and prevention,
- Distributed Denial of Service (DDoS) attack monitoring, mitigation, and alerts, and
- intelligence gathering and sharing.

Progress

Participation of state agencies and other eligible government entities in the statewide information security program is voluntary and can be limited by available funding. Where necessary, DIR utilizes a risk-based approach to provide services to eligible agencies.

Security Monitoring

DIR serves as the Internet Service Provider (ISP) for more than 150 Texas entities serving over 147,000 state employees. The purpose of the NSOC, established by Texas Government Code, Section 2059 in 2007, is to provide perimeter security for agency customers. The NSOC monitors more than 2.8 million public-facing Internet Protocol (IP) addresses owned by the State of Texas. In the role of an ISP, the NSOC also provides Denial of Service (DoS) and DDoS monitoring and mitigation for agency customers.

The NSOC has adopted a 3-step approach to protect the State's assets:

1. Block traffic to and from any known bad IP address or website,
2. Focus analysis on outbound traffic looking for malicious call outs, and
3. Gather evidence of the malicious traffic and alert the appropriate agency of the suspicious activity.

The NSOC operates an enterprise Network Intrusion Prevention System (NIPS). This system actively protects the State of Texas by blocking malicious network traffic. The NSOC must strike a strategic balance between aggressively blocking known bad IP addresses while allowing agencies to conduct state business through their critical applications. To better achieve this goal, the NSOC has developed highly beneficial cyber-intelligence sharing relationships. These relationships provide additional, reliable cybersecurity information for use with prevention and detection tools. In addition, NSOC blacklists any scanning, brute force login, vulnerability probing, or similar type of "threat reconnaissance traffic" detected by NSOC tools.

The NSOC protects state assets using a toolset designed to detect malicious communications, which inspects all traffic that enters and leaves the State of Texas' networks. DIR continues to invest in security tools and processes to maintain the appropriate level of security required to operate the state's Network Security Operations Center. At the outset of the COVID-19 pandemic, DIR doubled its' internet capacity to meet growing demand; however, the state's security posture was not compromised because the proper tools were in place to handle the extra load.

The NSOC provides DDoS network protection services for agency customers. DIR provides 24/7 DDoS detection and mitigation services for our state agency customers and internet circuits. The NSOC network providers detect and auto-mitigate volumetric attacks (a new type of DDoS attack) as they occur.

To further improve intelligence gathering and sharing capabilities, the NSOC participants in the Texas Information Sharing and Analysis Organization (TxISAO). The NSOC is currently participating in a Department of Homeland Security (DHS) funded pilot for automated intelligence exchange between state, local, territorial, and tribal governments. The NSOC regularly shares intelligence with our federal, state, and higher education partners.

Table 1 provides a list of the NSOC's fiscal year 2020 alerts to provide a better understanding of the types of malicious activity that occur. The top three categories – malware, DDoS, and suspicious activity – make up 89% of all alerts.

Table 1	
Threat Category	**Alerts**
Malware	77
DDoS	52
Suspicious Activity	28
Phishing	7
Ransomware	5
Miners	4
InfoStealer	3
Grand Total	**176**

The leading category, malware, is a generic malware group. Most of these detections were for malware variants that were a combination of a backdoor (a covert means for a third party to bypass traditional security and enter a system) and an effort to steal credentials to circumvent security measures. The second most common type of alert sent by the NSOC was for DDoS attacks. DDoS attacks have increased in frequency and impact. Traditionally, DDoS attacks mostly hampered the delivery of services to the public; however, with state employees working from home during the COVID-19 pandemic, an attack can also affect an employee's ability to connect remotely and perform work duties. The NSOC expects DDoS attacks to be prevalent as remote work continues.

The last of the top three threat categories is suspicious activity. NSOC investigates communications that look abnormal. If they prove to be malicious or highly suspicious, NSOC sends an alert to the agency. Phishing continues to be the delivery method of choice for bad actors. The NSOC started a program requesting that agencies send any suspicious emails to our NSOC analysts for analysis. This has proven very effective as the NSOC reviews dozens of emails and implements needed phishing website blocks each week.

Assessments

Technical Assessments

DIR provides agencies with no-cost technical security assessments. These assessments include network penetration tests, along with limited web and mobile application penetration tests, to evaluate network, systems, and web application security vulnerabilities. Agencies can purchase network vulnerability scanning and web application vulnerability scanning through DIR's Managed Security Services (MSS) program.

State Agency Security Program Assessments

DIR also utilizes the MSS program to provide comprehensive security and risk management assessments based on the Texas Cybersecurity Framework (TCF). These assessments are provided to state agencies, universities, and community colleges.

Table 2 shows the number of penetration tests and TCF assessments provided by DIR in 2019 and 2020.

Table 2: Assessments Provided in the Fiscal Years 2019 and 2020 Biennium				
Fiscal Year	**Penetration Tests**	**Web/Mobile Penetration Tests**	**TCF Assessments**	**Total**
2019	56	11	39	106
2020	55	13	41	109

Educational Services

DIR provides cybersecurity education and training to state agencies at no cost to the agency. These include DIR's annual Texas Information Security Forum and advanced technical cybersecurity training delivered through the Texas InfoSec Academy. DIR also provides other educational events including webinars, presentations, and workshops.

Table 3 shows the number of agencies participating in education offerings during the fiscal 2019-2020 biennium.

Table 3[1]: State Agencies, Universities, and Community Colleges Represented at Education Offerings	
FY2019	114 (out of 144)
FY2020	175 (out of 191)

Financial Consideration

Network security services are incorporated into the TEXAN services contract providing additional value for TEXAN customers. DIR has determined all state agencies that are part of the consolidated state network are paying their proportional cost of baseline NSOC security services

[1] Beginning September 1, 2019: Community Colleges were required to follow the security provisions in Texas Government Code, Section 2054, and became eligible for OCISO services – changing the number of active organizations from 144 to 191.