Report on the Consolidated Network Security System

2018 BIENNIAL PERFORMANCE REPORT

Texas Department of Information Resources

This report meets the requirements of Texas Government Code, Section 2059.057. It describes the consolidated network security system's accomplishment of service objectives and performance measures, including financial performance.

BACKGROUND

Cybersecurity is the protection of the confidentiality, integrity and availability of data and 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. The Texas Department of Information Resources (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 and coordinates with agencies to protect state information and elevate the security posture and capabilities of the state. The Office of the Chief Information Security Officer (OCISO) within DIR oversees the statewide information security program which includes:

- Cybersecurity governance, policy and planning
- Comprehensive security program risk assessments
- Technical security assessments including controlled penetration testing, web application and host vulnerability assessments
- Security education and training
- 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 a Network and Security Operations Center (NSOC), a secure and resilient facility with security operations co-located and integrated with statewide network management functions. The NSOC is tasked by the state legislature to provide 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 at the State of Texas through:

- Security event monitoring and analysis, alerting, and incident response coordination
- Network intrusion detection and prevention
- DDoS Attack monitoring, mitigation, and alerting

PROGRESS

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

SECURITY MONITORING

The Department of Information Resources (DIR) serves as the Internet Service Provider (ISP) for more than 150 State of Texas agencies and some Institutions of Higher Education. The purpose of the NSOC, established in 2007, is to provide perimeter security for our customers. The NSOC team keeps constant watch over a significant IP space. We protect and monitor more than 2.8 million public-facing IP addresses.

Each business day over 147,000 State of Texas employees use the DIR-provided internet. To protect their privacy and the integrity of customer data, our prevention and monitoring systems and procedures must be finely tuned to be available 24x7x365. To ensure that these services are always available, the NSOC provides Denial of Service (DoS) and Distributed Denial of Service (DDoS) monitoring and mitigation.

The NSOC also manages an Enterprise Network Intrusion Prevention System (NIPS). The NSOC must be strategic with the blocking that it provides to its customers, striking a balance between aggressively blocking known bad domains and IPs and providing reliable service. The NSOC has entered cyber-intelligence sharing relationships which provides collaborative cybersecurity information to be added into our prevention and detection tools. In addition, any scanning, brute force login, vulnerability probing, or similar type of threat reconnaissance traffic is blacklisted. The current number of blocks per month range from 20 to 30 billion! This means that 20-30 billion potentially malicious events are currently being stopped by the NSOC. These numbers illustrate how large our attack surface is and the volume of threats that we face daily at the NSOC. So how do we deal with protecting a network that large from so many different threat actors?

To answer this question let's examine the NSOC's alerts for fiscal year 2018:

NSOC Alerts for FY-2018

Alert Category	Alert Count
Suspicious Activity	88
Phishing	31
Miners	28
InfoStealer	20
Ransomware	14
Downloader/Backdoor	12
Worm/Botnet/Adware/etc.	5
DDoS	3
Hacking	1
GRAND TOTAL	**202**

The top categories here – Suspicious Activity, Phishing, and Miners – compose most of our alerts. The leading category, Suspicious Activity, is comprised of scanning, enumeration, and other intrusion attempts like DNS calls and random web shell upload attempts. This category also includes exploit kit activity and TOR usage. The Phishing category was our second most common alert which is no different than the private sector the same 12 months. The NSOC started a program requesting the agencies to send any suspicious emails to our NSOC analysts for analysis and counter-measure actions. This has proven very effective as we receive dozens of emails which lead to phishing website blocks each week. Miners is a new category to stay with the technology. Miners are considered very low risk, but they are a theft of State of Texas resources and therefore monitored. Credential theft and ransomware are still profitable and therefore are still prevalent attack vectors which we continue to defend against.

TECHNICAL ASSESSMENTS

DIR provides agencies with no-cost, technical security assessments including Controlled Penetration Testing (CPT), Web Application Vulnerability Scans (WAVS), and Vulnerability Assessments (VA) to evaluate network, systems, and web application security vulnerabilities. Table 2 shows the number of WAVS, CPTs and VAs provided by DIR in 2017 and 2018.

Table 2. Technical Assessments

Fiscal Year	Web Application Vulnerability Scans	Penetration Testing	Vulnerability Assessments	*TOTAL*
2017	3	49	11	***63***
2018	3	50	3	***56***

STATE AGENCY SECURITY PROGRAM ASSESSMENTS

DIR collaborates with an independent vendor to perform comprehensive security and risk management assessments of selected state agencies.

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 in 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 2017-2018 biennium.

FINANCIAL CONSIDERATION

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

Table 3. State Agency and Institution of Higher Education Represented at Education Offerings

Fiscal Year	Agency Participation
2017	122 (of 143)
2018	130 (of 143)