

Report on Consolidated Network Security System

2016 BIENNIAL
PERFORMANCE
REPORT

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. 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 cyberattacks.

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 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
 - Security event monitoring, analysis alerting and incident response coordination
 - Network intrusion detection and prevention
- 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 supports the statewide information security program and provides cost-effective services to all state agencies and other eligible state entities.

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

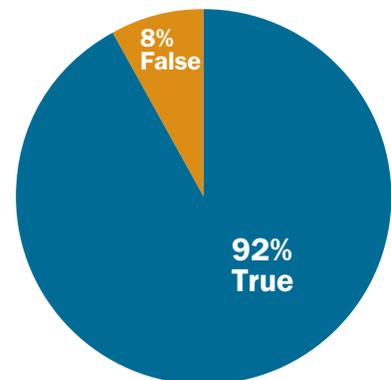
Progress

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

DIR performs network monitoring of state-managed and operated data networks and collaborates with a vendor to provide security services to eligible state agencies and entities at the NSOC. The NSOC currently has 153 customers. Through an aggressive blocking strategy that incorporates intelligence from multiple sources, the NSOC enterprise Intrusion Prevention System (IPS) averages 500 million blocks a week against malicious or unauthorized traffic directed toward State of Texas networks. The NSOC also employs multiple security tools to monitor traffic that is allowed to pass through its IPS. Any traffic that is deemed malicious or a potential indicator of a compromised host results in an alert being sent to the DIR customer. All alerts are tracked in the official state incident tracking system. Customer feedback is provided on the efficacy of these alerts via this incident tracking system. This allows the NSOC to gauge the effectiveness of its staff, its tools, and any new signature or filters that may be deployed on security tools. NSOC maintains a 92 percent true positive rate, or the rate of positive identified attacks, which means that the security monitoring and alerting is working as designed and is providing value to customers' security staff and programs.

Figure 1. True/False Positive Results for NSOC Alerts



Source: Statewide Portal for Enterprise Cybersecurity Threat, Risk and Incident Management



Report on the Consolidated Network Security System

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 1 shows the number of WAVS, CPTs and VAs provided by DIR in 2015 and 2016.

Table 1. Technical Assessments

Fiscal Year	Web Application Vulnerability Scans	Controlled Penetration Testing	Vulnerability Assessments	Total
2015	55	47	23	125
2016	56	48	3	107

State Agency Security Program Assessments

DIR collaborates with an independent vendor to perform comprehensive security and risk management assessments of selected state agencies. There were 21 assessments completed in FY 2015; none were completed in 2016 due to delays in the solicitation for this function. Delays were due to the creation of a new maturity benchmark framework based on the new Texas cybersecurity controls catalog that all agencies are now required to adhere to for each agencies cybersecurity plan. Although no assessments were performed in FY2016, the new award will return to regularly annual production levels in FY2017.

Educational Services

DIR provides cybersecurity education and training to state agencies at no cost to the agencies. 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 2 shows the number of agencies participating in education offerings during the FY 2015-2016 biennium.

Table 2. State Agency and Institution of Higher Education Represented at Education Offerings

Fiscal Year	Agency Participation
2015	118 (of 143)
2016	111 (of 143)