

Chief Operations Office (COO)
Deputy Executive Director's Office
Chief Procurement Office (CPO)

Network Security Operations' (NSO) Services

Internal Audit Public Report 17-102

January 2018



Department of Information Resources

Internal Audit Mission Statement

To collaborate with DIR leadership to fulfill the agency's core mission by providing independent and objective audit services designed to add value and improve the effectiveness of risk management, control, and governance processes.

DIR Internal Audit Staff

Lissette Nadal, CIA, CISA, CRISC, Director of Internal Audit

Ernst & Young LLP Advisors

Terry Jost, Southwest Region, Cybersecurity Leader
Doug Holt, Executive Director, Southwest Region, Government & Public Sector
Neill Masterson, Internal Audit Executive Director

Ernst & Young LLP Staff

James Merrill, CPA, CISA, Internal Audit Coordinating Executive
Valmiki Mukherjee, CISSP, CRISC, Cyber SMR, Executive Director
Audrey Hara, CISA, Internal Audit Manager
Teddy Abraham, CISSP, Cyber SMR, Manager
Douglas Maxham, CISSP, Cyber SMR, Senior

Executive Summary

The confidential audit report summarizes the scope, results, and recommendations from the work performed in conducting the Texas Department of Information Resources (DIR) Network Security Operations (NSO) services assurance audit. The assurance audit was included in the Fiscal Year 2017 Internal Audit Annual Plan.

The primary **objective** of the assurance audit was to assess whether the operations of the DIR network security function were in compliance with state law and regulations. In determining compliance with state law and regulations, the audit team assessed DIR’s compliance with 1) industry leading practices, 2) adoption of rules, 3) management, 4) services and support, 5) physical security, 6) training, and 7) contracted work. The audit team assessed the contractor’s compliance with relevant a) deliverables, and b) service level agreements (SLAs). In addition, the audit team also validated the implementation status of the audit recommendations included in the Chief Information Security Office (CISO)/ Network Security Operations audit report #13-105. The audit team also interviewed selected network security from a sample of state agencies to gain insight on the agencies’ perspective related to their roles and responsibilities over network security.

The **scope** of the audit included thorough research and investigation into the applicable policies and procedures that apply to the NSO services’ current operating model, as follows:

- Identified the Legislation, Government Code, and Directives that were available for deriving the scope of performance of the Network Security Operations Center (NSOC).
- Identified the operating Charter adopted by the NSO management for its current performance.
- Identified the applicable industry standard for NSO services that it would derive guidance from, in the form of NIST (National Institute of Standards and Technology) Special Publication 800-53, revision 4.

Summary of Results

Regulatory Compliance	Leading Practices Adoption/ Strategic	Management and Oversight	Policy and Procedures
2 Issues	3 issues	1 issue	2 issues

Recommendations to improve the NSO services controls were identified and communicated to DIR management who concurred with the results and recommendations reported by Internal Audit and provided action plans, estimated completion dates, and assigned responsibility to management staff for implementing the recommendations.

Network Security Operations

We conducted this performance audit in conformance with the *International Standards for the Professional Practice of Internal Auditing* and in accordance with the *Generally Accepted Government Auditing Standards*. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our issues and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our issues and conclusions based on our audit objectives.

Due to the confidential nature of the activity audited, a separate confidential audit report was provided to the DIR Board and executive leadership including the overall conclusion, issues, and recommendations identified¹. Management responses were requested from DIR executive leadership charged with governance and sufficient authority and responsibility for implementing the corrective actions planned to address the audit recommendations reported.

¹ **Government Auditing Standards (GAS)** Chapter 7: Reporting Standards for Performance, Sections 39-43 address the reporting of confidential and sensitive information.

Report Distribution

External Public Report Distribution

Texas Office of the Governor

Texas Legislative Budget Board

Texas State Auditor's Office

Texas Sunset Advisory Commission