

---

# ENTERPRISE SECURITY ASSESSMENT

Information Security and Privacy

State of Utah

---

## ENTERPRISE SECURITY ASSESSMENT

---

### EXECUTIVE SUMMARY

The Department of Technology Services (DTS) Office of Enterprise Information Security (EISO) under the direction of the Chief Information Officer (CIO) has developed and embraced an enterprise-wide effort to strengthen the State of Utah's information security posture. In support of this effort, the EISO is implementing a robust security program for all twenty-three State agencies within the Executive Branch (the State Enterprise).

A security vulnerability assessment, conducted between May and October 2007, cataloged applications and established initial system security classifications, conducted an executive risk interview, defined an enterprise risk model, and identified potential information security vulnerabilities and risks associated with the State Enterprise that could affect the confidentiality, integrity, and availability of information processed by the State.

A representative sample of servers was selected from each agency. The sample was statistically valid with the percentage of servers based on the number of servers and inherent risk of the agency. The sample size was determined by the EISO, with actual server selection made by agency DTS staff. A total of 1,795 hosts were reviewed from an external (Internet, wireless, modem) and an internal perspective. In addition, physical security and protection of information assets were reviewed at each site visited, and the physical and environmental protection controls were reviewed for selected data centers and rooms.

The overall effort provided a significant baseline of existing practices and vulnerabilities and forms the baseline for developing and improving future security practices in Utah agencies. The overall best practices orientation of the assessment provides the opportunity for the State to be in greater compliance with enterprise security best practices across a diverse range of agencies.

---

### DESCRIPTION OF THE BUSINESS PROBLEM

DTS encompasses information technology (IT) functions formerly located within 23 separate Executive Branch agencies. Information security functions traditionally were performed by each of the 23 agency IT groups. These IT groups were independent and loosely coordinated, resulting in an uneven security landscape applied in an unsystematic manner.

A comprehensive State enterprise-wide security assessment of information systems and assets had never been performed across all agencies. This lack of

an enterprise baseline, combined with the lack of risk-based management models, made the task of defining appropriate and reasonable information security controls for the State's information assets very difficult, if not impossible.

### Solution Description

A comprehensive assessment of the State's information systems and practices was undertaken to establish a baseline security landscape and design appropriate information classification and risk management programs.

### **Assessment Project/Task Objectives and Requirements**

The purpose of the project was to conduct an enterprise-wide security assessment of the information assets of the State of Utah's Executive Branch agencies and service provider. There were two major tasks in the assessment project:

#### 1. Technical Risk Assessment

- Cataloging and Categorization of Applications and Systems
- Initial Risk Assessment
- External Vulnerability Assessment
- Internal Vulnerability Assessment

#### 2. Business Risk Assessment

- Development of Risk Management Program
- Development of Data Classification Program

The objectives for each major task in the project were to:

- determine and present the current state of information security protection within the enterprise;
- define and detail possible actions to reduce or eliminate vulnerabilities;
- estimate the complexity, cost, and effort to implement corrective action recommendations; and,
- develop sustainable risk management and data classification programs.

The objectives were accomplished by the DTS Information Security Team and the contractor, with the major responsibility of the contractor being the direction, support, knowledge transfer, and training of the DTS Information Security Team.

Detailed results are confidential to the State. A statistical summary of effort for the assessment is summarized in the following table:

**Table 1: Statistical Summary of Effort**

<b>Activities</b>	<b>Number</b>	<b>Scope</b>
Agencies Reviewed:	23	100% of Enterprise
Business Risk Interviews Conducted	30	100% of Enterprise
Applications Cataloged	891	
Cataloging Interviews Conducted	46	
Assessment Review Meetings	63	Average of 3 meetings per agency
IP Addresses In Scope	1,946	
Total Servers Reviewed:	1,795	30-40% of Enterprise
Operating Systems Reviewed	44	
Phone Numbers Reviewed	3,514	
Facilities and Sites Reviewed	25	
Data Centers Reviewed	27	
Wireless Site Reviews	8	100% of Executive Branch Campuses
Files Inventoried and Reviewed	5,550,941	

Length of Time in Operation

The project began in May 2007 and was completed in October 2007. Implementation of specific changes to operational business processes from the findings is ongoing.

SIGNIFICANCE TO THE IMPROVEMENT OF THE OPERATION OF GOVERNMENT

A comprehensive State-wide/enterprise-wide security assessment of information systems and assets had never been performed across all agencies. This lack of an enterprise baseline, combined with the lack of risk-based management models, made the task of defining appropriate and reasonable information security controls for the State's information assets very difficult, if not impossible.

Performing the comprehensive assessment of the State's information systems and practices allows the State to establish a baseline security landscape and design appropriate information classification and risk management programs. Costs for security and levels of effort to establish and manage security will be more accurately identified and will be scoped more appropriately.

## BENEFIT OF THE PROJECT

The following items represent the key benefits of the information security assessment that have been realized, or are anticipated near term results of the overall effort.

- Establishment of an enterprise-wide baseline defining the current state of the security landscape.
- Identification of the gaps between the ideal baseline model and the current state.
- Establishment of a risk based decision system requiring executive management review of gaps and deciding which are unacceptable (needing remediation), avoidable, or acceptable.
- Establishment of an enterprise risk model defining a baseline threshold for risk.
- Creation of a reasonable enterprise security plan focused on the remediation of the identified unacceptable gaps.
- Creation of an enterprise program designed to reduce or avoid the cost to reconstruct/recover data and/or indemnify stakeholders due to security breaches or identity theft.
- Allocate security costs to areas of specific need within the enterprise and each agency, driven by clearly understood business requirements.
- Increase stakeholder (especially the citizens of the Utah) confidence and trust that their information is secure and access to it is authorized and managed effectively.
- Creation of standard processes and procedures to identify and effectively deal with issues and incidents.