Risk Analysis Report

for

DSHS Registry Plus (Reg+)

(for the Texas Cancer Registry Program Area)

May 14, 2013

CONFIDENTIAL

Acceptance

Name	Title	Signature	Date
Melanie Williams, Ph.D.	Manager, Cancer Epidemiology and Surveillance Branch		
Earnest Valle	Director, IT Application Development		
Ricardo Blanco	Director, IT Operations		
Kevin J. White	Chief Information Security Officer		

Table of Contents

1 Executive Summary 1
1.1 Observations 1
1.2 Business Impact 1
2 System 2
2.1 Scope of Assessment 2
2.2 Approach 2
2.3 Test Environment 3
3 Overall Security Risk 4
3.1 Security Risk Rating 4
3.2 Information Security Assessment, Awareness, and Compliance (ISAAC) Results 4
3.3 Controlled Penetration Test(CPT) Results 5
3.4 Web Application Vulnerability Scan (WAVS) Results 5
4 Information Security Assessment, Awareness and Compliance (ISAAC) 6
4.1 Objectives 6
4.2 TAC 202 Compliance 6
5 Controlled Penetration Test (CPT) 7
5.1 Overview 7
5.2 CPT Rating System 7
5.3 Targeted Systems 8
5.4 CPT Results 8
5.4.1 FTP 9
5.4.2 SSH 9
5.4.3 SMTP 9
5.4.4 DNS 10
5.4.5 HTTP 10
5.4.6 RPC 10
5.4.7 NetBIOS 11
5.4.8 RDP 11
5.4.9 RemotelyAnywhere 11
5.4.10 MS Directory Service 11
5.4.11 GMR Update Service 12
5.4.12 Microsoft SQL Server 12
5.4.13 Tivoli Monitoring Service 12
5.4.14 Tivoli Storage Service 13
5.4.15 Microsoft OLAP4 13
5.4.16 Symantec AntiVirus 13
5.4.17 Bindview-IS 14

5.4.18 BMC/Marimba Mgmt 14
5.4.19 JDWP 14
5.4.20 CASP 15
5.4.21 Unknown 16
6 Web Application Vulnerability Scan (WAVS) Assessment 17
6.1 Overview 17
6.2 WAVS Results 17
6.4 Medium Vulnerabilities 18
6.4.1 Cross-Site Request Forgery 18
6.4.2 Session Identifier Not Updated 19
7 Security Controls 20
7.1 Administrative Security Controls 20
7.2 Physical Security Controls 20
7.3 Technical Security Controls 20
8 Mitigation Strategy 21
8.1 Actions 21
8.2 Mitigation Table 21
Appendix A: Roles and Responsibilities 23
Appendix B: Risk Assessment Procedure 24
Background 24
Overview 24
Approach 24
Information Security Policies, Standards, and Regulations 25
Threats and Vulnerabilities 25
System Security Plans (SSPs) 25
Appendix C: ISAAC Results 26
Appendix D: Web Application Vulnerability Scan Results 28

1 Executive Summary

The DSHS Business Program, Information Security Office staff, and Denim Group Ltd. conducted an information security risk assessment of the DSHS Registry Plus (Reg+) (for the Texas Cancer Registry Program Area) application. The assessments performed were the Information Security Assessment Awareness and Compliance (ISAAC), a Controlled Penetration Test (CPT) and a Web Application Vulnerability Scan (WAVS) assessment. The ISAAC portion is a subjective assessment performed by the business program that examines system compliance with Texas Administrative Code (TAC) 202 requirements. The CPT is a battery of tests against the environment that identifies weaknesses in the servers and network infrastructure. The WAVS assessment dynamically analyzes the application and its environment utilizing automated and manual testing tools.

1.1 Observations

The Information Security Assessment, Awareness, and Compliance for Texas State Agencies (ISAAC) risk assessment rated the DSHS Registry Plus (Reg+) system 100% compliant with TAC 202.

The CPT discovered multiple open ports on each of the targeted servers. The risks from the open ports are mitigated by multiple layers of defense (firewalls and security devices) in place; the firewall prevents external access to all servers and ports except for the web tier servers on ports REDACTED to access the web application. These open ports should be reviewed and any unnecessary ports closed.

During the initial scans performed, over 1100 vulnerabilities were discovered. After working with the Centers for Disease Control, which owns the application, the code was updated and the number of defects reduced significantly (52). No high vulnerabilities remained in the final scans, and only a limited number of medium and low defects.

1.2 Business Impact

Per the ISAAC assessment, the DSHS Registry Plus (Reg+) systems meets the requirements of TAC 202 as 100% compliant.

The CPT scan revealed that there are many open ports, some with unidentified services, on each of the servers scanned. These ports, with the exception of the web application ports on the web tier servers, are only accessible from within the DSHS network. There is a low risk to these ports being accessed from outside the DSHS network.

The WAVS analysis uncovered numerous vulnerabilities; most of these were remediated and only a few remain. The vulnerabilities have been examined and present some limited risk to the application if not remediated. Findings have been provided to the Centers for Disease Control (CDC) for remediation. It is also recommended to limit the number of administrator accounts (both application and data center systems administrators) to minimize exposure of these application vulnerabilities.

Based on the results of the ISAAC, CPT and WAVS assessments, the overall security risk rating for the Cancer Registry Plus system is low.

2 System

DSHS performed assessments on the following HRI (Health Registries Improvement) application:

Application	Summary
Registry Plus	The Registry Plus suite of software components was provided by CDC to facilitate implementation of the National Program of Cancer Registries (NPCR). These software components for collecting and processing cancer registry data are compliant with national standards.

2.1 Scope of Assessment

The assessment reviewed several aspects of the applications' security:

- Input Validation
- Authentication
- Access Control
- Information Disclosure
- Session Management
- Data Protection
- Application Workflow

Additionally, the assessment reviewed the application's hardware infrastructure:

- Port Scanning
- Account Brute Force
- Scripts for Known Vulnerabilities

2.2 Approach

Perform Automated Application Scanning

Web Application Vulnerability Scanning (WAVS) was executed on the DEV/TEST environment webserver. IBM Rational AppScan was utilized for performing the automated scanning of the application.

Perform Penetration Testing

The BackTrack Linux suite of tools was used to perform the penetration testing against the targeted servers.

Penetration Testing Methodology:

1. System Discovery – Automated scans to identify the environment systems visible to the point of entry
    - Tools: NMAP to identify open ports on the servers. NMAP scripts were also run for the identified services. Results are documented in Section 5.4.
2. Baseline Testing – Testing against known device and server vulnerabilities and common configuration errors
    - Tools: ZAP
3. Targeted Testing – Verify the exploitability of known issues, explore high-risk areas
    - Tools: ZAP

2.3 Test Environment

Testers conducted a port scanning assessment on DSHS Registry Plus (Reg+)'s development/test (DEV/TEST) environment. The Reg+ system administrators configured this environment for testing and demonstration purposes with a minimum of configuration differences from the production environment. For purposes of the engagement, testers treated the application configuration as if it were identical to a production release.

NOTE: The Information Security Office recommends that for future testing, the configuration be replicated identically to the production environment or each difference and reason be clearly documented by the application development support team.

The Reg+ system administrators provided access to the Reg+ application by creating user accounts indicative of the available roles on the information systems. WAVS testing was performed primarily against the development/test environment, although some intermediate testing was performed on the production environment when the test environment was not available due to the need to debug problems induced by the PGP encryption solution rollout.

CPT testing was performed on the production environment servers. No CPT testing was performed against the DEV/TEST environments servers.

NOTE: The ISO recommends that (1) CPT tests be performed against the DEV/TEST servers and (2) WAVS be performed against the production webserver when the resources are available to ensure the results are consistent between the two environments.

3 Overall Security Risk

The determination of an Overall Security Risk Rating is based on the highest level of risk found during the course of the risk assessment. The severity levels used for this determination are discussed in the following sections:

- *Information Security Assessment, Awareness and Compliance (ISAAC)*
- *Controlled Penetration Test (CPT)*
- *Web Application Vulnerability Scans (WAVS) Assessment*

The overall security risk rating for DSHS Registry Plus (Reg+) is **Low**.

3.1 Security Risk Rating

System Information

Item	Description
Location of Servers	REDACTED
Number of Servers	8
Number of Windows Based Workstations	No dedicated workstations
Number of Users	~1,100
Value	$150,000
Classification	Confidential

Protection Need

Protection Need	Relative Need to Protect
Confidentiality	High
Integrity	High
Availability	Moderate

Overall Protection Need	High

3.2 Information Security Assessment, Awareness, and Compliance (ISAAC) Results

	Value	Compliant?
Texas Administrative Code (TAC) 202	100%	✓

# of Mitigation Items
0

3.3 Controlled Penetration Test(CPT) Results

Severity	Impact	Total Vulnerabilities
Low	Open ports were discovered on each of the servers tested. Since the test was performed inside the DSHS network, these items are mitigated because of the firewall in place; the firewall only exposes ports REDACTED externally on the following hosts: REDACTED	95

3.4 Web Application Vulnerability Scan (WAVS) Results

Scans produced the number of issues at the following levels of severity.

WAVS Severity Category	Impact	Vulnerabilities
High	Direct danger to your application, web server, or information	0
Medium	Threat through unauthorized access to private areas, though the database and operating system are not at risk	13
Low	Allow for unauthorized reconnaissance	34
Other	Issues you should know about, not necessarily security issues	5

4 Information Security Assessment, Awareness and Compliance (ISAAC)

4.1 Objectives

The ISAAC online risk assessment tool measures compliance with Texas Administrative Code - 1 TAC 202. Additionally, the assessment involves risk mitigation through the application of countermeasures according to the National Institutes of Health (NIH) methodology. See Appendix C for detailed results.

The Business System Owner completed the information security risk assessment in April 2012. IT staff provided assistance in completing the assessment. Upon completion of the assessment, Business System Owners and IT staff discussed the results and revised the assessment as appropriate.

4.2 TAC 202 Compliance

DSHS Registry Plus (Reg+)

Based on the information provided by departmental personnel, the protection afforded by the system meets 100% of the information security standards of Texas Administrative Code 202. The system also satisfies the minimum requirement for the Relative Risk Rating of 4.5.

5 Controlled Penetration Test (CPT)

5.1 Overview

The purpose of the CPT is to assess an agency's network infrastructure security. The assessment is accomplished by testing:

- Edge routers
- Public Internet devices
- Firewalls
- Internal routers or switches
- Internal servers and workstations

The CPT was conducted from March 23-27, 2012. The scope of the assessment included DSHS network connected systems. DSHS conducted the controlled penetration testing from the vantage point of an outside attacker, restricting its activity to security reconnaissance, vulnerability analysis, and limited exploits of areas deemed most vulnerable. Once the external testing was completed, testing was performed within the internal network to emulate possible actions of an inside attacker.

DSHS used the following objectives to evaluate the test results for both internal and external networks:

- Ability to identify and retrieve proprietary information
- Ability to establish control of resources, such as network devices and servers

5.2 CPT Rating System

Severity	Description
High	High risk vulnerabilities are those that may allow access to the affected host, with the potential result of loss of data, exposure of confidential information or further access into the network. Also included in this category are vulnerabilities to denial−of−service attacks that can cause a system to hang or crash. All high risk vulnerabilities should be corrected immediately.
Medium	Medium risk vulnerabilities allow attackers to mask their activities using DSHS systems, or make activities and systems appear as if they are the attacker. Also included in this category are vulnerabilities to any activities that cause annoyance, such as mild denial−of−service attacks that use unnecessary bandwidth but do not completely eliminate access.
Low	Low risk vulnerabilities are those that may provide information about the host or network that is not inherently dangerous but may compromise DSHS privacy policy or would be useful in an attack.

5.3 Targeted Systems

Host Name	IP Address
Production Environment	
REDACTED	REDACTED
REDACTED	REDACTED
REDACTED	REDACTED
REDACTED	REDACTED
Development/Test Environment	
REDACTED	REDACTED
REDACTED	REDACTED
REDACTED	REDACTED
REDACTED	REDACTED

5.4 CPT Results

Vulnerability	Impact	Severity
5.4.1 FTP	REDACTED.	Low
5.4.2 SSH		Low
5.4.3 SMTP		Low
5.4.4 DNS		Low
5.4.5 HTTP		Low
5.4.6 RPC		Low
5.4.7 NetBIOS		Low
5.4.8 RDP		Low
5.4.9 RemotelyAnywhere		Low
5.4.10 MS Directory Service		Low
5.4.11 GMR Update Service		Low
5.4.12 Microsoft SQL Server		Low
5.4.13 Tivoli Monitoring Service		Low
5.4.14 Tivoli Storage Service		Low
5.4.15 Microsoft OLAP4		Low
5.4.16 Symantec AV		Low

5.4.17 Bindview-IS		Low
5.4.18 BMC/Marimba Mgmt		Low
5.4.19 Java Debug Wire Protocol		Low
5.4.20 CASP		Low
5.4.21 Unknown		Medium

5.4.1 FTP

Host Name	Port(s)	Service Name
REDACTED	REDACTED	File Transfer Protocol (FTP)

Description
File Transfer Protocol is used to transfer files to authenticated or anonymous users. FTP services verify username and password, but the credentials are transmitted over the network in plain text. An attacker can steal the FTP login information by placing a network sniffer somewhere along the connection path, such as on the FTP server local area network (LAN) or on the client LAN.

Secure FTP (SFTP) services allow authenticated users to transfer files over an encrypted connection.

5.4.2 SSH

Host Name	Port(s)	Service Name
REDACTED	REDACTED	Secure Shell (SSH)
REDACTED REDACTED REDACTED	REDACTED	

Description
Secure Shell is a network protocol for secure data communication, remote shell services or command execution and other secure network services between two networked computers – a server and a client – that it connects via a secure channel over an insecure network.

5.4.3 SMTP

Host Name	Port(s)	Service Name
REDACTED	REDACTED	Simple Mail Transfer Protocol (SMTP)

Description
The Simple Mail Transfer Protocol specification allows for a mail system to relay or direct email to a recipient by forwarding messages through an intermediate mail server. Any organization with an open mail relay allows unauthorized persons to use disk space and bandwidth to send electronic junk mail or advertising. Spammers often use this technique to hide their identities.

5.4.4 DNS

Host Name	Port(s)	Service Name
REDACTED	REDACTED	Domain Name System (DNS)

Description
The Domain Name System is a hierarchical distributed naming system for computers, services, or any resource connected to the Internet or a private network. The DNS service routes TCP host name requests to the IP address assigned.

5.4.5 HTTP

Host Name	Port(s)	Service Name
REDACTED	REDACTED REDACTED	Hypertext Transfer Protocol (HTTP)
REDACTED REDACTED	REDACTED	
REDACTED REDACTED REDACTED	REDACTED REDACTED REDACTED REDACTED REDACTED REDACTED	
REDACTED	REDACTED REDACTED	

Description
The Hypertext Transfer Protocol is an application protocol for distributed, collaborative, hypermedia information systems. The HTTP is an application-level request/response protocol that uses extensible semantics and MIME-like message payloads for flexible interaction with network-based hypertext information systems.

5.4.6 RPC

Host Name	Port(s)	Service Name
REDACTED REDACTED REDACTED	REDACTED REDACTED	Remote Procedure Call (RPC)

Description
A remote procedure call is an inter-process communication that allows a computer program to cause a subroutine or procedure to execute in another address space (commonly on another computer on a shared network) without the programmer explicitly coding the details for this remote interaction.

5.4.7 NetBIOS

Host Name	Port(s)	Service Name
REDACTED REDACTED REDACTED	REDACTED	Network Basic Input/Output System (NetBIOS)

Description
NetBIOS provides services related to the session layer of the OSI model allowing applications on separate computers to communicate over a local area network.

5.4.8 RDP

Host Name	Port(s)	Service Name
REDACTED REDACTED REDACTED	REDACTED	Remote Desktop Protocol (RDP)

Description
Remote Desktop Protocol (RDP) is a proprietary protocol developed by Microsoft, which provides a user with a graphical interface to another computer. The server listens on TCP port REDACTED by default.

5.4.9 RemotelyAnywhere

Host Name	Port(s)	Service Name
REDACTED REDACTED REDACTED	REDACTED REDACTED	Remotely Anywhere

Description
RemotelyAnywhere is a remote administration tool that lets you control and administer Microsoft® Windows®-based computers over a local area network or the Internet. RemotelyAnywhere acts as the host software on the machine that is to be controlled or accessed. The client requires no special software. RemotelyAnywhere provides such useful capabilities as Java-based desktop remote control, file transfer protocol (FTP) for downloading and uploading of files, configuration of the Host, remote-to-local printing, and advanced scripting.

This service is likely used by the Data Center Services contractor. This should be confirmed, along with the need, and should be configured according to best security practices for this software.

5.4.10 MS Directory Service

Host Name	Port(s)	Service Name
REDACTED REDACTED REDACTED	REDACTED	Microsoft Directory Service

Description
Directory services are used for network administration and security to authenticate and authorize all users and computers in a Windows domain type network—assigning and enforcing security policies for all computers and installing or updating software.

Four Common Vulnerability and Exposures (CVEs) were reported in the National Vulnerability Database for Microsoft Directory Services for Server 2003. Apply all recommended corrective and mitigation actions.

5.4.11 GMR Update Service

Host Name	Port(s)	Service Name
REDACTED	REDACTED	gmrupdateserv

Description
GMR Update Services is used by programs to exchange data directly, instead of going through a file or other temporary storage location.

No CVEs were found in the NVD for this protocol. Further checks should be made to determine if this protocol is used by the Registry Plus application or any Data Center Services applications. Some indications exist that this protocol is vulnerable to Denial of Service attacks, but this should be mitigated for those servers behind the firewall. Unless absolutely essential, this service should be closed on the webserver.

5.4.12 Microsoft SQL Server

Host Name	Port(s)	Service Name
REDACTED	REDACTED	ms-sql-s

Description
Microsoft SQL Server 2008 is a data management and analysis solution that delivers increased security, scalability, and availability to enterprise data and analytical applications, while making them easier to build, deploy, and manage.

Seventeen CVEs were reported in the National Vulnerability Database for Microsoft SQL Server 2008.
Verify the need for its use and ensure that is configured according to best security practices. Apply all recommended corrective and mitigation actions.

5.4.13 Tivoli Monitoring Service

Host Name	Port(s)	Service Name
REDACTED	REDACTED REDACTED REDACTED REDACTED	IBM Tivoli Monitoring
REDACTED	REDACTED REDACTED REDACTED	
REDACTED	REDACTED REDACTED REDACTED REDACTED REDACTED REDACTED	

Description
Likely used by the Data Center Services contractor to monitor the performance and availability of distributed operating systems and applications. These products are based on a set of common service components, referred to collectively as Tivoli Management Services. Tivoli Management Services components provide security, data transfer and storage,

notification mechanisms, user interface presentation, and communication services in an agent-server-client architecture

Four CVEs were reported in the National Vulnerability Database for Tivoli Monitoring for DB2 as distributed in IBM DB2 9.7 (and other/earlier variants).
Verify the version installed and confirm its necessity. Apply all recommended corrective and mitigation actions.

5.4.14 Tivoli Storage Service

Host Name	Port(s)	Service Name
REDACTED REDACTED REDACTED	REDACTED	Tivoli Storage Manager (http interface)

Description

A total of 38 CVEs were reported for versions 6.2 and earlier of Tivoli Storage Manager.
Verify the version installed and take appropriate action if version 6.2 or earlier is in use.

5.4.15 Microsoft OLAP4

Host Name	Port(s)	Service Name
REDACTED	REDACTED	ms-olap4

Description
Online analytical processing (OLAP) allows access of aggregated and organized data from business data sources, such as data warehouses, in a multidimensional structure called a cube. Microsoft SQL Server 2008 Analysis Services (SSAS) provides tools and features for OLAP used to design, deploy, and maintain cubes and other supporting objects.

No CVE found in the National Vulnerability Database.

5.4.16 Symantec AntiVirus

Host Name	Port(s)	Service Name
REDACTED REDACTED REDACTED	REDACTED	symantec-av

Description
Port REDACTED is extensively used by Symantec Antivirus for client-server communication. This port can be manually configured by the user when the system is under a proxy or a secured network connection.

Though not confirmed by the NVD, port REDACTED reportedly may also be used by an IRC Bot variant Trojan to infiltrate a remote computer through the SYMCO06-010 exploit. The port is used by the malware to initiate DDoS and packet flooding attacks on remote computers using the same port as a backdoor.
Review and ensure that this service is required.

5.4.17 Bindview-IS

Host Name	Port(s)	Service Name
REDACTED	REDACTED	bv-is

Description
A directory administration, vulnerability management and policy assessment & management software providing customers with the tools to assess, discover and remediate network, hardware or application anomalies.

Bindview-IS and bv-is are not found in the National Vulnerability Database. Bindview, in versions from 2002 and earlier, are noted with various vulnerabilities.
Verify the version installed and take appropriate action if this version is from 2002 or earlier.

5.4.18 BMC/Marimba Mgmt

Host Name	Port(s)	Service Name
REDACTED REDACTED REDACTED	REDACTED	BMC/Marimba Management

Description
BMC's Marimba software provisioning and distribution products enable enterprises to rapidly respond to changing business requirements by re-purposing, re-provisioning, and updating IT resources to achieve required IT configurations. Marimba configuration discovery and tracking products enable enterprises to track both the state and usage of their hardware and software assets.

No CVE found in the National Vulnerability Database. This service is likely used by the Data Center Services contractor. This should be confirmed, along with the need, and should be configured according to best security practices for this software.

5.4.19 JDWP

Host Name	Port(s)	Service Name
REDACTED REDACTED REDACTED	REDACTED	Java Debug Wire Protocol (JDWP)

Description
Java Debug Wire Protocol (JDWP) defines communication between debuggee (a Java application) and debugger processes. It is a component of the Java Platform Debugger Architecture, a collection of APIs used to debug Java code.

No CVE found in the National Vulnerability Database. This service is likely used by the Data Center Services contractor. This should be confirmed, along with the need, and should be configured according to best security practices for this software.

5.4.20 CASP

Host Name	Port(s)	Service Name
REDACTED REDACTED REDACTED	REDACTED	Connection Administration Control (CAC) App Service Protocol (CASP)

Description
In a connection-oriented network, the role of CAC is to decide whether there are sufficient free resources on the requested link to allow a new connection. A connection can only be accepted if sufficient resources are available to establish the connection end-to-end with its required quality of service. The agreed quality of service of existing connections in the network must not be affected by the new connection. If the network has the required resources, the CAC may allow a connection request to proceed; if not, the CAC will indicate this and notify the originator of the request that the request has been refused.

No CVE found in the National Vulnerability Database. This service is likely used by the Data Center Services contractor. This should be confirmed, along with the need, and should be configured according to best security practices for this software.

5.4.21 Unknown

Host Name	Port(s)	Service Name
REDACTED REDACTED	REDACTED	Unknown
REDACTED	REDACTED	

Description
The services running on these ports are unknown. The assessment scanned each of these ports in an attempt to determine the service operating on the port. The services running on these ports did not match any of the common TCP ports, services or interfaces; some of the ports appear to be configured for SSL. Services running on them may be used by the Data Center Services contractor. This should be confirmed, along with the need, and should be identified, documented, and then configured according to best security practices for each protocol/service using the port.

Each of these ports should be reviewed to ensure that there are necessary services listening on each port and closed if not needed.

6 Web Application Vulnerability Scan (WAVS) Assessment

6.1 Overview

DSHS uses IBM's Rational® AppScan® to test all components of an application that is Web-based or URL-based. A Rational AppScan Full Scan consists of two stages: Explore and Test.

Explore stage: During this stage, the site is explored and an application tree is constructed. AppScan analyzes the responses to each request it sends, looking for any indication of a potential vulnerability. When AppScan receives responses that may indicate security vulnerability, it automatically creates tests, as well as noting the validation rules needed to determine which results constitute vulnerability, and the level of security risk involved.

Test stage: During this stage, AppScan sends thousands of custom test requests that it created during the Explore stage. It records and analyzes the application's response to identify security problems and rank their level of security risk.

The DSHS Information Security Team administers a complete test, which runs thousands of tests based on all levels of typical user techniques as well as unauthorized access and code injections. See Appendix D for detailed results.

It is preferable to conduct the web application vulnerability testing against a test or mirrored site to avoid any disruption of production systems.

Due to the nature of the AppScan software (under default settings) it is possible to saturate the computer(s) hosting the targeted URL(s) with external communications requests, so that it cannot respond to legitimate traffic, or responds so slowly as to be rendered effectively unavailable. The scan could force the computer(s) hosting the web application to reset, or consume its resources; especially Java processes, so that is cannot provide its intended service. Also, system logging may be stopped or logs may be overwritten due to resource consumption.

6.2 WAVS Results

DSHS performed WAVS scans of both the production and development/test webservers.

The initial scans conducted were of the development/test webserver, REDACTED, using three different User IDs. One of these identities was configured to evaluate if privileges could be escalated to perform functions that should be restricted to administrators. As a result of these scans, we discovered a significant number of vulnerabilities.

Due to the high number of defects (1130 in all), these findings were provided to the Center for Disease Control (CDC) for action, since the Registry Plus application is their software product provided for DSHS use. CDC made several iterations of changes to the application, after which additional scans were performed by Denim Group and ISO staff on the application. These final scans have been reviewed and the defects identified in them have been deemed of low risk to the system. However, these defects have been reported to CDC for their remediation.

NOTE: Defects that remain, though not considered critical, have been reported to the CDC for remediation. When CDC provides an update to the application code, Reg+ should be rescanned to ensure these defects have been remediated to DSHS satisfaction.

The table that follows shows the original number of defects AppScan discovered by user ID.

Registry Plus Initial WAVS Defects Summary

Scan Titles	Privilege Escalation	Sec_Central_ Admin	Sec_Facility (aka Abstractor)
Vulnerability Levels			
High	136	20	7
Medium	18	81	31
Low	96	283	132
Information	35	206	85

Current AppScan defects (as of May 17, 2012) based on the latest code updates from CDC.

Registry Plus Final WAVS Defects Summary

Scan Titles	Privilege Escalation	Admin (aka sec_central_admin)	Abstractor (aka Sec_Facility)
Vulnerability Levels			
High	0	0	0
Medium	7	5	1
Low	16	6	12
Information	5	0	0

The following sections provide a general, brief review of the types of medium severity defects that were common across all the WAVS scans. Low and Informational categories are not addressed in the body of this report; these details are available in the final WAVS reports, which are found in Appendix D.

6.4 Medium Vulnerabilities

Medium vulnerabilities fell into the following two categories: Cross-Site Request Forgery and Session Identifier Not Updated.

6.4.1 Cross-Site Request Forgery

With Cross-Site Request Forgery, it is possible to steal or manipulate customer session and cookies, which might be used to impersonate a legitimate user, thus allowing the hacker to view or alter user records and to perform transactions as that user.

Reasoning:

The same request was sent twice in different sessions and the same response was received. This shows that none of the parameters are dynamic (session identifiers are sent only in cookies) and therefore that the application is vulnerable to this issue.

Comments:

Analysts probed each of these reported vulnerabilities under a regular login session and could not find an exploit that led to an exposure of confidential or private health information.

6.4.2 Session Identifier Not Updated

When a Session Identifier is not updated, it is possible to steal or manipulate customer session and cookies, which might be used to impersonate a legitimate user, thus allowing the hacker to view or alter user records and to perform transactions as that user.

Reasoning:

One or more session identifiers were not updated in the response.

Comments:

Analysts probed each of these reported vulnerabilities under a regular login session and could not find an exploit that led to an exposure of confidential or private health information.

7 Security Controls

7.1 Administrative Security Controls

Information Security Policy	✓
Information Security Standards and Guidelines	✓
Computer Usage Policy	✓
Computer Usage Handbook	✓
Computer Usage Agreement	✓
Security and Computer Usage Training and annual recertification	✓
Information Security Awareness (Notices, Articles and Guidance)	✓
Computer Incident Response Plan	✓
Information Security Team	✓

7.2 Physical Security Controls

Guards are on duty	✓
There is a receptionist on duty	✓
Visitors are escorted	✓
Identification is required for personnel	✓
Building - Environmental monitoring controls	✓
Building - Fire Protection and Suppression System	✓
Building - Badges	✓
Building - Access Card Locks	✓
Building - Two layers	✓

7.3 Technical Security Controls

Vulnerability scanning is performed on the system	✓
Symantec Endpoint Protection	✓
System patches and fixes implemented as a result of new releases, patches, and vulnerabilities discovered/remediated	✓
Data access requirements, authorizations, permissions and rights approval are performed by system owner.	✓
Audit trails are captured by the Registry Plus application and perimeter security devices	✓

8 Mitigation Strategy

8.1 Actions

Texas Administrative Code 202 states that, "The state agency head or his or her designated representative(s) shall make the final security risk management decisions to either protect the data or accept exposures according to its value/sensitivity."

By 6/30/13

8.2 Mitigation Table

CPT				
Issue/Risk	**Recommendation**	**Management Decision**	**Timeline**	**Cost**
REDACTED	REDACTED			$0.00
REDACTED	REDACTED	REDACTED		$0.00
WAVS		REDACTED		
Issue/Risk	**Recommendation**	**Management Decision**	**Timeline**	**Cost**
REDACTED	REDACTED			$0.00
REDACTED				$0.00
TAC 202 Compliance				
Issue/risk	**Recommendation**	**Management Decision**	**Timeline**	**Cost**
No issues	N/A	N/A	N/A	N/A

Security Policy Compliance				
Issue/Risk	**Recommendation**	**Management Decision**	**Timeline**	**Cost**
System Security Plan (SSP)	The Information Security Office will support the Business Owner to create the SSP for Reg+ within 45 days of entry into production operations.	Complete SSP with ISO support	By 5/31/13	$0.00

Appendix A: Roles and Responsibilities

Information System Owner

This person is the key point of contact for the DSHS Registry Plus (Reg+) and is responsible for coordinating system development life cycle activities specific to the system. This person is the senior management official who has the authority to authorize (accredit) operation of an information system and accept the residual risk associated with the system.

Name	Melanie A. Williams, Ph.D.
Title	Branch Manager, Texas Cancer Registry
E-mail Address	Melanie.Williams@dshs.state.tx.us
Phone Number	512-305-8092

System/Security Custodian

The following person is assigned responsibility for the DSHS Registry Plus (Reg+) /security of the subject system:

Name	Blas Galaviz
Title	Group Manager, IT AppDev
E-mail Address	blas.galaviz@dshs.state.tx.us
Phone Number	512-776-6003

Appendix B: Risk Assessment Procedure

Background

Texas Administrative Code (TAC) 202 Information Security Standards and the Department of State Health Services (DSHS) Information Security Policy require that risk assessments be performed on information resources. Annual risk assessments are required on all high-risk systems. Medium and low-risk systems require biennial risk assessments.

Overview

The information security risk assessment:

- assesses the risks to the agency's information assets
- provides a qualitative and quantitative analysis of the effectiveness of the current security controls that protect the assessed system
- identifies the threats to and vulnerabilities in the information system
- identifies and analyzes the security controls for the information system
- provides the basis for a risk-based decision for selecting security controls

DSHS Information Technology (IT) incorporates the use of three components in its risk assessment process to obtain a greater analysis of the DSHS Information Resources (IR) environment:

- **Information System Assessment, Awareness and Compliance (ISAAC):** Evaluates the effectiveness of current security controls and compliance with state law and best practices. It relies on the judgment of the Business System Owner and IT staff to determine the overall risk of the information system.
- **Controlled Penetration Test (CPT):** Tests the network and infrastructure for vulnerabilities in the following:
  - Edge routers
  - Public Internet devices
  - Firewalls
  - Internal routers or switches
  - Internal servers and workstations

  The CPT is conducted by the Department of Information Resources (DIR) on an annual basis.
- **Web Applications Vulnerability Scan (WAVS):** Tests for vulnerabilities in the application and coding if the system is Web-based or URL-based.

Approach

The information risk assessment is a qualitative and quantitative analysis of the effectiveness of current security controls that protect the assessed information system. The assessment process consists of four phases.

1. **Assessment**. The Business Owner completes the ISAAC with assistance from IT Staff as needed, DIR performs the CPT, and Information Security staff perform a WAVS assessment if applicable.
2. **Data Analysis**. Business Owners meet with IT staff to discuss the results of the ISAAC, and revise the assessments as appropriate. Information Security staff meet with Application Development staff to discuss the results of the CPT and the WAVS.
3. **Mitigation Strategy**. This phase consists of determining and enacting the appropriate processes or security controls to reduce risk to an acceptable level.

4. **System Security Plan (SSP)**. An important activity during this phase is documentation. A System Security Plan (SSP) for the information system explains the security requirements, how controls are implemented, and how they are to be maintained.

Information Security Policies, Standards, and Regulations

The most relevant information security policies, standards, regulations, and guidelines with which the information system must adhere are:

- Texas Administrative Code (TAC) 202, Information Security Standards
- Health and Human Services Enterprise Security Policy, Standards and Guidelines
- Department of State Health Services (DSHS) Information Security Policy
- DSHS Information Security Standards and Guidelines
- DSHS Internal Audits

Threats and Vulnerabilities

The following table shows possible threats to information security, how the threat is implemented, and the impact of the threat.

Threats and Vulnerabilities

Threats	Vulnerabilities	Impact
Hackers, terminated employees, unauthorized users	Unauthorized Access	May cause disclosure, modification, destruction, or loss of information
User with authorized access.	Integrity checks and audit trails not maintained appropriately	May cause a harmful occurrence, either intentionally or unintentionally
Environmental hazards	Faulty hardware, faulty software, an unanticipated power outage, surge, lightning, water damage, fire, tornado, humidity, heat	May cause loss of availability, destruction, or modification of information
Malicious code or malware	System security updates and patches not applied in a timely manner	May cause loss of availability, disclosure, modification, destruction, or loss of information

System Security Plans (SSPs)

The assessment of risk and the development of SSPs are two important activities in an agency's information security program that directly support security accreditation. The SSP explains the security requirements, how controls have been implemented, and how they are to be maintained.

Texas Administrative Code 202 states that "Security requirements shall be identified, documented, and addressed in all phases of development or acquisition of information resources." Also, business owners must "Specify appropriate controls, based on risk assessment, to protect the state's information resources from unauthorized modification, deletion, or disclosure."

An SSP is recommended for each system to become fully compliant with TAC 202 security documentation rules. IT staff provide templates, guidance, and assistance to the business system owners in completing the necessary documentation.

SSPs should be developed within 12 months.

Appendix C: ISAAC Results

The ISAAC Risk Assessment for the Registry Plus system has been REDACTED.

Appendix D: Web Application Vulnerability Scan Results

This appendix contains 3 separate WAVS scans.

- Abstractor w95 ! / ¢95 Security Report
- Administrator w95 ! / ¢95 Security Report
- Privilege Escalation w95 ! / ¢95 Security Report

Abstractor Scan Report represents the Central Registry Abstractor/Reviewer role, which reviews abstract submitted by hospitals and doctors' offices for completeness and accuracy; compares text in the abstract against codes submitted to make sure they are the correct codes; corrects any errors or discrepancies found; also abstracts new cases.

Administrator Scan Report represents the Central Registry Administrator, who sets up the local facilities with access to the Web Plus software to report their data; creates a configuration for the facilities and defines their required fields and validation rules.

Privilege Escalation Scan Report is the scan where attempts were made to escalate privileges from the lower level abstractor to that of the system administrator.

Due to the length and technical content of the full detailed reports, the reports contained here are summaries. Copies of the detailed reports, as well as the raw scan output files, are available by contacting the Information Security Office.

The names of these reports are:

- w95 ! / ¢95
- w95 ! / ¢95
- w95 ! / ¢95

The WAVS reports has been REDACTED.