OFFICE OF THE MINNESOTA SECRETARY OF STATE

Steve Simon

December 31, 2015

2015 Legislative Report of Security of Online Voter Registration and Absentee Ballot Application Tools

COST OF REPORT PREPARATION

Estimated costs are provided in accordance with Minnesota Statutes, section 3.197:

> A report to the legislature must contain, at the beginning of the report, the cost of preparing the report, including any costs incurred by another agency or another level of government.

The total cost for the Office of the Secretary of State to prepare this report was approximately $2,833. These costs are exclusively staff time needed for gathering the data, completing and reviewing test results, responding to any items from the test results, and preparing the written report.

OVERVIEW

Minnesota law requires the Office of Secretary of State to engage in an annual security assessment of the online voter registration and absentee ballot application tools, and submit a report of the assessment to the Legislative Auditor and chairs and ranking minority members of the committees in the Senate and House of Representatives with primary jurisdictions over elections. Minn. Stat. §§ 201.061, subd. 8; 203B.04, subd. 7; and 203B.17, subd. 3 (2014). Reports are due by January 1 of each year.

The Office of the Secretary of State conducted an annual security assessment of the online voter registration and absentee ballot application tools utilizing Veracode, a third-party security firm, as well as reviewing the internal practices employed to ensure the security of the online tools. On December 30, 2015, Secretary of State Steve Simon signed the certification that adequate security measures are in place.

In early 2016, the Office of the Secretary of State will be releasing an updated version of the Office's webpage, which will include updates to the online voter registration and online absentee ballot application tools. The Office will perform the same security tests on the updated online tools prior to the release of the new online tools, and will submit a supplemental report to the Legislature and the Legislative Auditor.

SECURITY ASSESSMENT

Security of Online Registration and Absentee Ballot Application Tools

Security in the Technical Development of the Online Tools

The Office of the Secretary of State developed the online voter registration tool, absentee ballot application tool, and UOCAVA (military and overseas voters) absentee ballot application tool between approximately March 2013 and September 2013. The development of these online tools was done in conjunction with other updates to the Statewide Voter Registration System (SVRS). In developing these tools, the Office consulted with staff at MN.IT on both the design approach and potential security issues. Based on input from MN.IT, the Office made adjustments to the overall coding design. Included in the design is a requirement that all data transmitted through these tools be encrypted.

Prior to launching the online voter registration tool and UOCAVA absentee ballot application tool in 2013, the Office contacted MN.IT regarding a security assessment of the online tools. MN.IT referred the Office to Veracode, a third-party web application security firm. Veracode is used by MN.IT and other state agencies in assessing the security of web-based applications. Additional information on Veracode is attached to this report.

The Office chose to run the online tools through the maximum Veracode protocols and sought a security score of 90 or higher. A score of over 90 is considered the highest security standard.

The Office ran the online tools through the Veracode scan on two different occasions prior to the launch of the online tools. The Veracode scan identifies security issues and categorizes them into risk categories: very high, high, medium, low, and very low. The first scans of the online tools using Veracode identified several items of medium risk, but no items of high or very high security risk. The Office made changes to the application based on the issues identified by Veracode, and ran a subsequent Veracode scan to ensure that the issues had been corrected. The subsequent Veracode scan returned no high or very high security risks, and returned an overall security score of 94.

The 2014 Legislative Report of Security of Online Voter Registration and Absentee Ballot Application Tools indicated in the narrative that there were no “medium or higher” risks. As reflected in the accompanying documents to the report, contrary to the narrative there were 12 medium risks identified by the Veracode scan. Office IT staff and the Office security infrastructure manager reviewed the medium risks and determined that they did not pose a security risk due to framework and validation methods that mitigated the identified medium risks. An explanation of the mitigating framework and validation methods is contained in Appendix I.

The Office also ran WebInspect, another security and vulnerabilities tool, against both the Office’s online tools prior to the launch of the tools. WebInspect categorizes any security issues into categories: critical, high, medium, low, information, and best practices. Again, the

WebInspect scan did not identify any critical issues, but did identify one high and one medium risk issue. The Office made changes to the online tools to correct the high and medium issues identified by WebInspect.

The Office then launched both the online voter registration tool and the UOCAVA absentee ballot application tool on September 23, 2013. The Office waited to launch the absentee ballot application tool for non-UOCAVA until the start of no-excuse absentee voting in May 2014. In advance of the general election, the Office revised the online tools to improve their usability on mobile devices. This revision did not change the underlying coding and structure of the online tools, but instead only changed the tools' outward appearance to users. The Office again ran a Veracode scan against the revised version of the online tools. This scan was run on August 29, 2014, and produced a score of 94, the same score as the tools received in September 2013.

2015 Security Assessment

In December 2015, the Office again performed a Veracode scan on the current version of the online voter registration and online absentee ballot application tools. This scan produced a score of 96. A score of over 90 is considered the highest security standard. The scan identified no high or very high risks, but identified nine medium risks. As with the medium risks identified in 2014, Office IT staff and the Office security infrastructure manager reviewed the medium risks and determined that they did not pose a security risk due to framework and validation methods mitigating the identified medium risks. An explanation of the mitigating framework and validation methods is contained in Appendix I.

In December 2015, MN.IT performed a WebInspect scan of the current versions of the online voter registration and online absentee ballot application tools. The WebInspect scan returned two issues identified as critical. Office IT staff determined that the first critical issue identified is a false positive. The second critical issue is being addressed and will be resolved in January 2016. A further explanation of the issues identified by the WebInspect scan is contained in Appendix J.

Security in the Processing of Applications Submitted Through the Online Tools

In addition to the technical design of the online tools, the Office designed the tools to ensure that the same or increased security measures were in place in relation to the online application processing as compared to the processing of paper applications. For example, the same procedures use to verify paper voter registration and absentee ballot applications are used in the online systems:

- Local election officials still need to review each record;
- Each voter who updates his or her registration or newly registers is sent a non-forwardable Postal Verification Card; and
- All online records receive the same standard eligibility checks, including comparisons to data from the Department of Corrections, the Courts, the Department of Public Safety, and the Department of Health.

In addition to these standard verification procedures used in both the online and paper systems, the online voter registration system has an additional verification requirement that any registration be verified against a government database before being queued through SVRS for review and processing by local election officials.

Monitoring of the Internet Protocol Address Log and Usage Volume

The Office maintains a log of each Internet Protocol address used to submit an online voter registration and online absentee ballot application, and reviews those logs for suspicious activity. The Office also reviews applications that failed verification against a government database for indicators of suspicious activity. This review includes, but is not limited to, reviewing those applications for suspicious activities such as fictitious looking names (e.g. "Mickey Mouse"), same name numerous times, and multiple applications at the same address.

Security of all Online Systems

In addition to these pre-launch security measures, the Office engages in ongoing security monitoring and best practices security for all of its web-based tools and resources. This includes the use of firewalls, secondary and concurrent layer protection, ongoing intrusion protection, regularly scheduled security scans for vulnerabilities, encryption of data, utilizing isolated databases, and ongoing analysis of the system logs for abnormal activity. If abnormal activity is found, the source IP address is then denied at the firewall. These additional security measures protect the whole of the Office's online tools, including the online absentee ballot and voter registration application tools.

SECURITY DATA PROVIDED TO THE LEGISLATIVE AUDITOR

In accordance with *Minnesota Statutes*, Chapter 13, the Office may only provide the legislature with data classified as public, and must withhold or redact any data classified as private, non-public, or confidential. The Legislative Auditor, however, is entitled to access all data in the Office, regardless of the data classification. The Office has provided the Legislative Auditor with this report, and has supplemented this report with additional information that is non-public due to its classification as security data. The Office's Security Declaration is attached to this report.

The additional information provided to the Legislative Auditor is outlined in the attachments list below, and includes the full Veracode scan results and WebInspect scan results, as well as additional details regarding the specific security protocols built into the online tools.

CONCLUSION

Based on the evaluation by technical staff and test results from third-party security organizations, the Secretary of State has certified that there are adequate security measures in place to safeguard the online voter registration and online absentee ballot application tools. The signed determination of the adequacy of security protocols is attached to this report.

Appendix

A. Determination by the Secretary of State of the Adequacy of Security Protocols
B. Statement from Veracode Regarding Accuracy of Assessment
C. Fact Sheet Prepared by Veracode
D. Data Sheet Prepared by Hewlett-Packard on WebInspect
E. Office of Secretary of State Security Declaration
F. Supplemental Addendum of OSS Security Procedures (Provided to Legislative Auditor Only)
G. Veracode December 7, 2015 Testing Results (Provided to Legislative Auditor Only)
H. WebInspect December 29, 2015 Testing Results (Provided to Legislative Auditor Only)
I. Supplemental Addendum of OSS review of Medium Risks identified by Veracode scan (Provided to Legislative Auditor Only)
J. Supplemental Addendum of OSS review of Critical Issues identified by WebInspect scan (Provided to Legislative Auditor Only)

A.

Determination by the Secretary of State of the Adequacy of Security Protocols

STATE OF MINNESOTA
Office of the Minnesota Secretary of State
Steve Simon

December 30, 2015

CERTIFICATION OF ADEQUACY OF SECURITY PROTOCOLS

Minnesota law requires the Secretary of State to annually certify that "adequate security measures are in place" to ensure the security of the Office of the Secretary of State's online voter registration and absentee ballot application tools. Minn. Stat. §§ 201.061, subd. 8; 203B.04, subd. 7; and 203B.17, subd. 3 (2014). Based on the evaluation by technical staff and test results from third-party security organizations, I certify that adequate security measures are in place to safeguard the online voter registration and online absentee ballot application tools.

Steve Simon

Secretary of State Steve Simon

Date: 12/30/15

180 State Office Building | 100 Rev. Dr Martin Luther King Jr Blvd | Saint Paul, MN 55155
Phone: 651-201-1324 or 1-877-600-8683 | Fax: 651-296-9073 | MN Relay Service: 711
Email: Secretary.state@state.mn.us | Web site: www.sos.state.mn.us

B.

Statement from Veracode Regarding Accuracy of Assessment

VERACODE

Julie Strother
Secretary of State
State of Minnesota

September 24, 2014

Dear Julie,

Thank you for your request regarding your recent scan of your application using our Static Analysis solution. Based on that scan we submit the following:

The results of the SAST scan are accurate in relation to the protocols chosen by the Office of Secretary of State.

Please let us know if we can be of further assistance to the State of Minnesota.

Best regards,

Chris Wysopal
Chief Technology Officer
Veracode, Inc.

65 Network Drive • Burlington, MA 01803 • Office 339.674.2500 • Fax 339.674.2502

C.

Fact Sheet Prepared by Veracode

VERACODE | FACT SHEET

CUSTOMER SUCCESS EXAMPLE:

For a Global 2000 enterprise, Veracode delivered the following results:

- ✔ **Grew testing program to cover over 1000 custom applications**
- ✔ **Assessed over 100 application builds every month**
- ✔ **Increased application portfolio coverage at an unprecedented pace**
- ✔ **Remediated and verified over 650,000 flaws in one year**
- ✔ **Reported on program success and progress versus industry peers**

Our SAST technology identifies critical vulnerabilities such as SQL injection, cross-site scripting (XSS), buffer overflows, unhandled error conditions and potential back-doors. It classifies and prioritizes the vulnerabilities.

Binary Static Analysis

Identify and fix security threats earlier. Get to market faster.

Unique in the industry, our patented binary static application security testing (SAST) technology analyzes all code — including third-party components and libraries — without requiring access to source code.

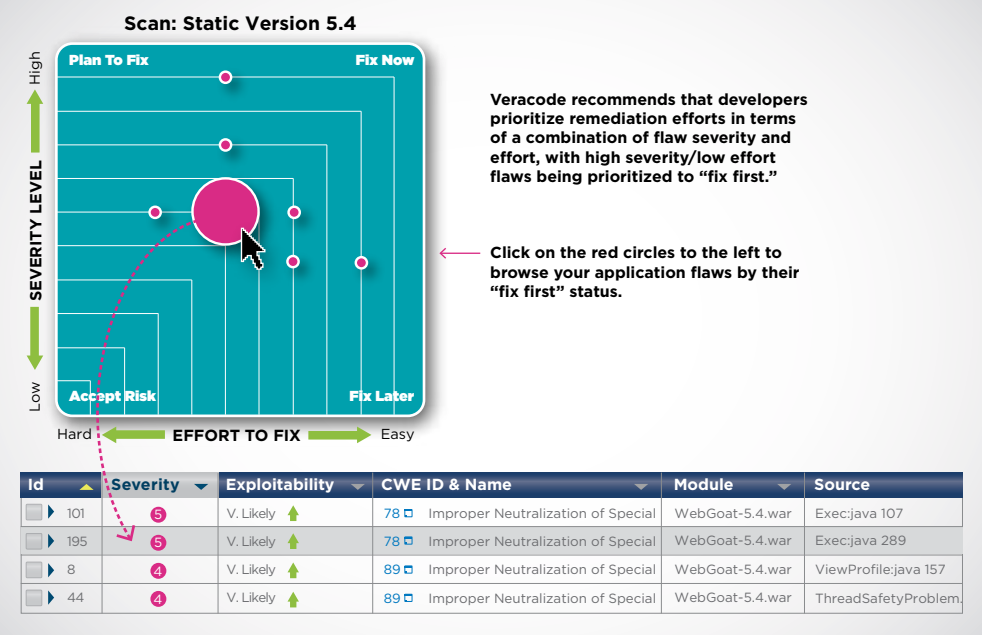
SAST supplements threat modeling and code reviews performed by developers, finding coding errors and omissions more quickly and at lower cost via automation. Our technology is typically run in the early phases of the Software Development Lifecycle because it's easier and less expensive to fix problems before going into production deployment.

Our SAST technology identifies critical vulnerabilities such as SQL injection, cross-site scripting (XSS), buffer overflows, unhandled error conditions and potential back-doors. It classifies and prioritizes the vulnerabilities using standard NIST severity levels. Actionable information is delivered to help developers address them quickly, including detailed remediation information.

How Binary SAST Works

Binary SAST analyzes binary code to create a detailed model of the application's data and control paths. The model is then searched for all paths through the application that represent a potential weakness.

For example, if a data path through the application originates from an HTTP Request and flows through the application without validation or sanitization to reach a database query, then this would represent a SQL Injection flaw.



VERACODE

FACT SHEET

HIGHLIGHTS

Most regulatory bodies and industry organizations recommend or require static analysis as a critical control to reduce application-layer risk, including:

- ✔ **FS-ISAC: Financial Services Information Sharing and Analysis Center**
- ✔ **Council on Cyber Security: Critical Infrastructure**
- ✔ **PCI Security Standards Council**
- ✔ **OWASP OpenSAMM**
- ✔ **SANS: Critical Security Controls**

Binary SAST Delivers Deep Visibility

Our binary SAST technology makes it faster than ever to find and fix vulnerabilities in your applications. It delivers detailed information that:

Is accurate: Static binary analysis examines applications the same way attackers look at them: By creating a detailed model of the application's data and control flows. Unlike legacy source code scanners, this approach accurately detects hidden threats such as backdoors that are difficult to detect because they're not visible in source code.

Is actionable: Prioritized results can be accessed via standard bug tracking systems such as JIRA or Bugzilla or viewed through our web interface. Flaw details and remediation advice are automatically provided to aid in rapid mitigation or remediation.

Minimizes false positives: Legacy scanning tools have a reputation for generating a high volume of vulnerabilities, which lowers productivity because of the time required to identify false positives. Our centralized platform is backed by world-class security experts and continuously learning with every new application it scans, to reduce false positives so you can start remediating faster.

Built on a Centralized, Cloud-Based Platform

Our binary SAST technology is fully integrated with our central cloud-based platform. This enables you to aggregate, analyze and share results with all stakeholders in a single dashboard, including:

- Results obtained via multiple techniques (SAST, dynamic analysis and manual penetration testing).
- Reports on remediation efforts and compliance with your custom policies.
- Security analytics and peer benchmarking to measure the progress of your global application security program.

Our cloud-based platform is continuously learning to adapt to evolving threats and reduce false positives; massively scalable to address your global application infrastructure; and a central part of Veracode's programmatic, policy-based approach for systematically reducing application-layer risk compared to traditional ad hoc approaches.

The platform integrates seamlessly with development processes and tools including:

- IDEs including Visual Studio and Eclipse
- Build servers such as Jenkins, Ant, Mave, Team Foundation Server (TFS)
- Issue tracking systems like JIRA, Bugzilla and RSA Archer GRC

When combined with our scalable cloud-based platform and programmatic, policy-based approach, binary SAST enables you systematically reduce application-layer risk across your global infrastructure — without slowing down your developers.

Veracode has assisted hundreds of development teams and software vendors overcome their resistance to developing secure code.

To learn more, visit: www.veracode.com/products

Veracode's cloud-based service is a simpler and more scalable way to reduce application-layer risk across your entire global software infrastructure — including web, mobile and third-party applications — without hiring more consultants or installing more servers and tools. With Veracode's smart approach to application security, you can drive your innovations to market faster — without sacrificing security in the process. Backed by world-class application security experts and a Magic Quadrant Leader since 2010, our cloud-based platform safeguards web, mobile and third-party applications for more than 500 organizations worldwide, including 3 of the top 4 banks in the Fortune 100 and 25+ of the world's top 100 brands.

VERACODE
The Most Powerful Application Security Platform on the Planet

D.

Data Sheet Prepared by Hewlett-Packard on WebInspect

Data sheet

HP WebInspect

Identify exploitable security vulnerabilities in web applications and services.

The leader in web application security assessment

HP WebInspect is the industry-leading web application security assessment solution designed to thoroughly analyze today's complex web applications and web services for security vulnerabilities. It delivers broad technology coverage, fast scanning capabilities, extensive vulnerability knowledge, ease of use, and accurate web application scanning results.

Enable broader lifecycle adoption through security automation

The earlier in the development process that security vulnerabilities are discovered, the less expensive they are to fix. HP WebInspect gives security professionals and security novices alike the power and knowledge to quickly identify and validate critical, high-risk security vulnerabilities in applications running in development, QA, or production.

Innovations of HP WebInspect include:

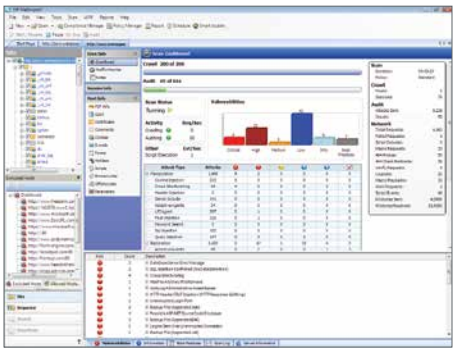
JavaScript/Ajax: HP WebInspect technology will trace and record code paths through JavaScript, fully analyzing how the application changes from the user's perspective as well as watch the Ajax and web service requests and then make attacks to the server-side application accordingly to reveal vulnerabilities.

Adobe® Flash: HP WebInspect addresses security vulnerabilities that exist within applications using Adobe Flash technologies by decompiling Flash files and performing static analysis on the resulting code to detect vulnerabilities.

Web Service: HP WebInspect employs a specific set of algorithms to detect Web Services and capture URL rewriting business logic. WebInspect then attacks all relevant URL parameters and determines the presence of security vulnerabilities.

Accelerate security through more actionable information
HP WebInspect doesn't just discover security vulnerabilities that someone else needs to fix, it interactively communicates the security knowledge needed to reproduce and fix discovered issues. Through cooperation with other HP Fortify solutions and integrations with HP Quality Center and HP Application Lifecycle Management, HP WebInspect's first-class knowledge base provides comprehensive details about the vulnerability detected, the implications of that vulnerability if it were to be exploited, as well as best-practices and coding examples necessary to quickly pinpoint and fix the issue, all published in the developer's defect management solution.

Guided Scan functionality: WebInspect's new Guided Scan functionality greatly enhances testing results by augmenting WebInspect's scanning technology with the information it needs to pinpoint application security vulnerabilities. Just as tax preparation software lets you prepare a tax return without understanding the nuances of the IRS, Guided Scan functionality lets you optimize a scan without having to know the details about the application under test and yet still receive the best application security assessment possible.



WebInspect dashboard
Dashboard delivers real-time visibility into and interactivity with test results.

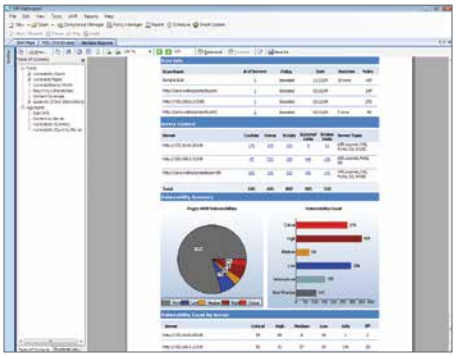
Find more vulnerabilities and fix them faster with HP WebInspect Real-Time

HP WebInspect Real-Time is a bundled application security solution that combines the advanced dynamic application security testing technology of HP WebInspect with the runtime application security technology of HP Fortify SecurityScope for dramatically improved scan results over previous dynamic application security testing approaches.

When used in conjunction with HP Fortify SecurityScope, HP WebInspect Real-Time can stimulate an application through automated, external security attacks, and then gather internal, code-level vulnerability information by observing the attacks in the code as they happen in real time. HP WebInspect Real-Time identifies and crawls more of an application to expand the coverage of the attack surface and detect new types of vulnerabilities that can go undetected by siloed security testing technologies.

Elevate security knowledge across the business
HP WebInspect has the most powerful reporting system available, delivering a fast, flexible, and scalable instrument for communicating meaningful results from your application security assessment. In addition to the many standard report templates, HP WebInspect's simple report designer allows you to develop and generate fully customized reports that deliver the relevant knowledge to key stakeholders in a professional and polished format. HP WebInspect can also include data from external sources, providing full enterprise-grade reporting. HP WebInspect also features interactive vulnerability review and retest features that enhance the security team's ability to validate discovered issues and regression test fixes from development. This closed feedback loop from security testing through development improves the overall security effectiveness of application teams.

Comply with legal, regulatory, and architectural requirements
Along with the increase in web application attacks there are now many additional legal, regulatory, and best practice requirements related to application security. HP WebInspect gives you the capabilities to easily address these additional requirements in a cost-efficient manner. HP WebInspect includes detailed reports that show how your web applications meet government regulations and industry standards, as well as what changes are required for compliance. In addition, users can create new policies or customize existing ones. The sophisticated reporting system allows you to easily create, modify, or enhance the information reported. HP WebInspect includes pre-configured policies for every relevant regulation, and best practices including the Payment Card Industry Data Security Standard (PCI DSS), OWASP Top 10, ISO 17799, ISO 27001, Health Insurance Portability and Accountability Act (HIPAA), and many more.

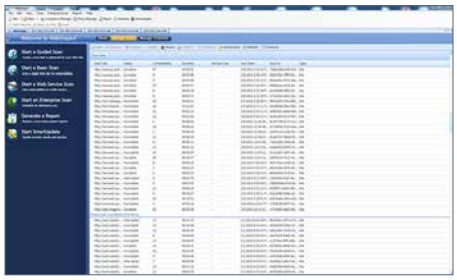


WebInspect Trend Reporting
View and analyze vulnerability trends over time to track application security progress and efficiency.

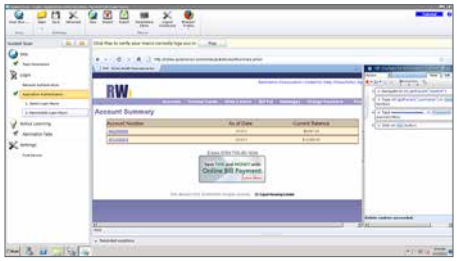
Leverage automation to do more with less
Every organization is faced with the challenges of doing more with less. HP WebInspect delivers the ability to drive significant results in the most efficient way. With the combination of the intuitive usability, intelligent scanning engines, first-class knowledge base, concurrent scan execution, live scan results, a tabbed workspace, and superior reporting, HP WebInspect helps you maximize the use of your valuable time, lower the cost of security vulnerability assessment and remediation, while reducing the risk of your web applications to your business.

Build an enterprise-wide application security program
HP WebInspect Enterprise gives you dynamic application-security testing that enables delivery of timely application-security intelligence across your entire enterprise no matter the size. The web-based interface establishes a shared security service and extends security testing to a larger audience. Distributed architecture, remote sensor technology, scheduling, and control capabilities support simultaneous scanning of many applications—when and where it makes the most sense for your business. As well, the WebInspect product suite integrates seamlessly with HP Software Security Center, letting your organization centralize and correlate results from static and dynamic testing as well as any testing results provided by our professional services organization, Fortify on Demand.

HP Software Security Research group
All HP Fortify Software Security Center solutions, including HP WebInspect, are informed by the expertise and threat intelligence from the HP Software Security Research group. This team's extensive research not only provides the latest innovations in web application vulnerability assessment but also automatically generates regular and timely updates to all products via HP SmartUpdate.



WebInspect Scan Database
Easily manage, view, and share your security test results and history



WebInspect Guided Scan
Guided Scan lets you optimize a scan without having to know the details about the application under test.

Key features and benefits

Innovative assessment technology

- Advanced client-side scripting technology to analyze JavaScript, Flash, and others
- Produce faster scans and more accurate results through simultaneous crawl and audit and concurrent scanning
- Advanced macro recording technology and flexible authentication handling for improved session management in complex applications
- Increase accuracy of detection using intelligent engines designed to imitate a hacker's methodology
- Innovative application architecture profiler assists in tuning the scan configuration and recommends improvements in site coverage and accuracy
- List-driven assessments for targeted and efficient application scanning
- Fingerprinting of web framework using Smart Scan technology to reduce unnecessary attacks

HP WebInspect Real-Time

- Integrated dynamic and real-time analysis to find more vulnerabilities and fix them faster
- Works in concert with HP Fortify SecurityScope to observe attacks at the code level during dynamic scans
- Identify and crawl more of an application to expand the coverage of the attack surface and detect new types of vulnerabilities
- Provides stack traces and line-of-code detail to confirmed vulnerabilities

Interactive vulnerability review and management

- Publish results to HP Software Security Center and quickly understand how they changed from scan to scan
- Streamlined vulnerability review process enables user to interact with test results
- Flexible vulnerability results view for grouping and filtering of results
- Displays detailed steps to reproduce a vulnerability and show how it was identified
- Retest a single vulnerability by re-executing the series of steps to validate or regression test a fix
- Enter manual findings and attach screenshots and documents to test results for better context and communication
- Retest Vulnerabilities functionality greatly reduces remediation validation time by retesting previously discovered vulnerabilities and providing confidence measurements that they have been accurately addressed
- Persist test results across scans

Advanced web services security testing

- Support for complex data types for rendering advanced WSDLs and specifying test data
- Automatically discover and audit web services embedded in an application
- Focused web service attacks and fuzzing
- Web Service Security Designer tool for configuring web service security tests

Refined and simple usability

- Quickly initiate simple or regression scans with minimal configuration for immediate results
- Walk through an intuitive wizard to set up a scan and begin reviewing results within seconds
- Review and control multiple simultaneous scans and reports through a tabbed interface
- Submit false positive reports and other feedback directly and securely to HP in just a few clicks
- Create reusable, componentized macros to record testing steps and login procedures

Resources, contacts, or additional links

To know more about how HP Fortify can resolve your application security concerns, visit
hp.com/go/fortify

Actionable remediation and compliance reports

- Run compliance reports for all major regulatory standards, including PCI, SOX, ISO, and HIPAA.
- Create flexible, extensible, and scalable reports that match your business.
- Simplify repetitive report generation through report templates.
- Assess application security trends and readiness.
- Scan comparison allows for the delta analysis comparison of vulnerabilities across two scans.

Key integrations

- Integrate into your defect management processes with out-of-the-box integrations with HP Application Lifecycle Management and Quality Center
- Integrate into your enterprise application security management process with an out-of-the-box integration with HP WebInspect Enterprise and HP Assessment Management software
- Extensive data export via XML for open integration with other security management systems
- Include information from external data sources in your reports via ODBC, SQL, or XML connections

About HP Enterprise Security

HP is a leading provider of security and compliance solutions for the modern enterprise that wants to mitigate risk in its hybrid environment and defend against advanced threats. Based on market-leading products from HP ArcSight, HP Fortify, and HP TippingPoint, the HP Security Intelligence Platform uniquely delivers the advanced correlation, application protection, and network defenses to protect today's hybrid IT infrastructure from sophisticated cyber threats.

HP Services

HP ESP Global Services take a holistic approach to building and operating cyber security and response solutions and capabilities that support the cyber threat management and regulatory compliance needs of the world's largest enterprises. We use a combination of operational expertise—yours and ours—and proven methodologies to deliver fast, effective results and demonstrate ROI. Our proven, use-case-driven solutions combine market-leading technology together with sustainable business and technical process executed by trained and organized people.

Learn more about HP ESP Global Services at
hpenterprisesecurity.com

Sign up for updates
hp.com/go/getupdated

Share with colleagues

Rate this document

4AA1-5363ENW, February 2013

E.

Office of Secretary of State
Security Declaration

OFFICE OF THE MINNESOTA SECRETARY OF STATE

SECURITY INFORMATION DECLARATION

Officewide

Purpose

The purpose of this policy is to classify the type of data in the possession of the Office of the Secretary of State and define what Minnesota law permits as "security information" under the classification of data. (Section 13.37, subd. 1 and 2), while complying with all Minnesota Statutes and ensuring that no such internal system information leaves the office that could result in a security risk.

Declaration

The Office of the Secretary of State (OSS) possesses a large amount of data, specifically computer programming of systems upon which the "domain data" resides. These computer programs are neither data on individuals nor data covered by other specific data practices classifications. For example, data on specific voter registrations are covered in Minnesota Election Law, most specifically section 201.091, which makes certain data public only for certain purposes. Data on specific business entities on file with OSS are public data. Data on Uniform Commercial Code (UCC) filings are public data.

The computer software and associated information are crucial to the security of domain data—both public and private or non-public, to the operation of the voter registration and business services systems as well as the internal accounting operations of the office.

The Information Technology staff of the Office has indicated that the data residing on the computing systems in the OSS are divided into two types of data; domain data and system data.

1. Domain Data

As an example, OSS Systems such as the Statewide Voter Registration System (SVRS) contain domain data, such as Voter Information, Address Ranges, and Polling Places. Much of these data can be ordered as a Public Information List. Processes are in place to extract and deliver this information under the appropriate, authorized circumstances. In the event that a Data Practices Act request includes such data, reports are run or queries created to extract data as long as the request does not include non-public data such as, but not limited to, voter information not included in the public information list.

2. System Data

In the design, building and testing of a system, specific data is created that is defined for purposes of this classification as "System Data". This includes certain aspects of database designs, programming code, test scripts, test results data, security and development methodology information. This type of data is security information classified as non-public data, with the exceptions indicated in paragraph 3, in order to protect system security and data integrity. Most applications at OSS are web-based applications, which are accessible outside of OSS. This requires additional protection of the data described in this declaration. The public disclosure of most of the data defined as "System Data" in paragraph 3 would constitute a security risk due to the fact that it may provide internal database design information, security methodology information, or other data about the technology that could be used by intruders to assist in unauthorized access of "domain data" in the system.

3. Security Information

For the foregoing reasons, the types of data listed in a) to i) below are defined as "System Data" and are declared to be security information as defined in Minn. Stat. section 13.37. Therefore that information must not be disclosed to the public, except to the extent of the exceptions described after each bullet point listed below, for each type of data. However, if the totality of a request is perceived by OSS to create a security risk under that section, even this information is declared to be security information and therefore non-public.

a) Application Design Data:

Database designs, except:

- Operating Systems (SQL Server, Microsoft Access, Oracle) may be disclosed.
- Transactional or Reporting data structure design approach may be disclosed.

Programming design, except:

- Design Patterns may be disclosed.

High-level architectural design data, except:

- Design Patterns may be disclosed.

System Requirements documentation, including notes, except:

- Hardware profiles including the number of CPUs and RAM may be disclosed.

System contextual design data, except:

- Data Dictionary documents may be disclosed.

System interface designs to other agencies or systems, except:

- OSS may disclose interactions with other agencies or systems via WPF Services, WCF Services, FTP, etc. but no specifics on implementation of how they are being used may be disclosed.

b) Application Programming data:

Database tables, stored procedures, views, designs, scripts

Development platform, tools used, except:

- Platform information (e.g., ASP.NET Framework 4.0, MVC 4) may be disclosed.

Programming Languages (e.g., C#, VB, MAPPER), except:

- The language an application was developed may be disclosed.

System configuration files and scripts

Batch processing files and scripts, except:

- OSS may disclose which items are processed in batch and which are processed one at a time.

c) Application Development Processes:

Design and coding policies, guidelines, processes, standards

Security design and coding policies, guidelines, processes, standards

Design and Security methodologies

d) Application Testing:

Test cases and scripts, except:

- The general approach for unit testing, web testing and load testing may be disclosed.

Test data used for test cases and scripts.

Testing results data, except:

- general chronologies of testing events including general descriptions of the event outcomes may be disclosed.

Testing tools and platforms, except:

- The name of tools used for testing (e.g.,Veracode, Webinspect and .NET Test Suite) may be disclosed.

Reports and details of issues or issues found in testing

e) OSS Computer Systems Infrastructure:

Hardware and software configuration information

Network Architecture and connectivity information, except:

- The fact that Firewalls, Intrusion Appliances, and similar programs are in use may be disclosed. Implementation methods of these tools must not be disclosed.

Disaster Recovery plans, tests, test data

Network Security plans, processes

f) OSS Computer Systems Network Administration:

Network user names, account, and password information

Network directory structures, file server names and addresses

Hardware maintenance data, such as security patches and upgrades

Processes and procedures such as system backup and recovery data

Physical computer facility information, such as location and number of sites

g) Application Support Documentation

Tickets related to the use of an application, where the details provide data about the system design.

User manuals, guides or notes that provide screen shots or other information that could be used in accessing the system, except:

- Release notes issued to counties when new versions are implemented may be disclosed.

User names, passwords, used in an application.

h) Project Management Information

Project Charters, plans and overviews

Project Schedules and release information

Reports and lists of features, enhancements, and issues resolved, except:

- General statements about and lists of feature enhancements, reports and issues resolved may be disclosed after new versions have been implemented.

Steering committee notes and release plans

Requirements data, including external system interfaces and agreements

i) Information Technology Policy Information:

Operational Policies, Procedures, and supporting data and reports

Security design and coding policies, guidelines, processes, standards

Disaster recovery and Business Continuation plans, policies

This declaration is effective from and after November 26, 2013 and supercedes the previous security information declaration adopted August 11, 2006.

Date: November 26, 2013

Mark Ritchie, Secretary of State

F.

Supplemental Addendum of OSS Security Procedures

(Provided to Legislative Auditor Only)

G.

Veracode Testing Results

(Provided to Legislative Auditor Only)

H.

Webinspect Testing Results

(Provided to Legislative Auditor Only)

I.

Supplemental Addendum
OSS Review of Risks Identified by Veracode

(Provided to Legislative Auditor Only)

J.

Supplemental Addendum
OSS Review of Risks Identified by WebInspect

(Provided to Legislative Auditor Only)