OFFICE OF THE MINNESOTA SECRETARY OF STATE

Steve Simon

December 28, 2017

2017 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 $1,067. 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 (2016). 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 27, 2017, Secretary of State Steve Simon signed the certification that adequate security measures are in place.

SECURITY ASSESSMENT

Security of Online Registration and Absentee Ballot Application Tools

Security in the Technical Development of the Online Tools and Previous Assessments

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. 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 Office also ran WebInspect, another security and vulnerabilities tool, against both of the Office's online tools prior to the launch of the tools. The Office chose to run the additional WebInspect scan because the WebInspect scan engages in a Dynamic scan analysis of the tools – as opposed to the purely Static scan analysis conducted by Veracode. 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 voters 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. As reflected in previous legislative reports, the Office of the Secretary of State has engaged in an annual review of the security of the online tools, and has reported the results of the review as required by Minnesota Statutes.

2017 Security Assessment

In November of 2017, the Office performed a Veracode scan on the current version of the online voter registration and online absentee ballot application tools. In previous years, the Veracode scan only provided a Static scan analysis of the online tools. However, starting in 2017 the Office was able to perform both Dynamic and Static scan analysis of the online tools through Veracode. Because the Office could now perform both a Dynamic and Static scan analysis of the online tools through Veracode, the Office did not utilize a secondary scanning service to provide a now-redundant Dynamic scan analysis.

The Veracode scan produced a Static scan score of 100 and a Dynamic scan score of 99. A score of over 90 is considered the highest security standard. The scan identified no high, very high, or medium risks, but identified four low risks and one risk identified as "informational." As with the risks identified in previous years, Office IT staff and the Office security infrastructure manager reviewed the identified risks. All of the risks identified by the Veracode scan were determined by Office IT staff to be false positives. An explanation and analysis of each identified risk can be found in Appendix A to the Veracode report.

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, 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 a third-party security organization, 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. Office of Secretary of State December 30, 2015 Security Declaration
D. Supplemental Addendum of OSS Security Procedures (Provided to Legislative Auditor Only)
E. Veracode November 22, 2017 Testing Results (Provided to Legislative Auditor Only)

A.

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

STATE OF MINNESOTA
Office of Minnesota Secretary of State
Steve Simon

December 27, 2017

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 the absentee ballot application tools. Minn. Stat. §§ 201.061, subd. 8; 203B.04, subd. 7; and 203B.17, subd. 3 (2016). Based on the evaluation by technical staff and test results from a third-party security organization, I certify that adequate security measures are in place to safeguard the online voter registration and online absentee ballot application tools.

Steve Simon

Steve Simon, Secretary of State

Date: 12/27/17

180 State Office Building | 100 Rev. Dr. Martin Luther King, Jr. Blvd. | Saint Paul, MN 55155-1299
Phone: 651-201-1324 or 1-877-600-8683 | Fax: 651-215-0682 | MN Relay Service: 711
E-mail: 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.

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

D.

Supplemental Addendum of OSS Security Procedures

(Provided to Legislative Auditor Only)

E.

Veracode Testing Results

(Provided to Legislative Auditor Only)