Maryland State Board of Elections
Online Voter Services
Vulnerability Assessment and
Penetration Testing Report

December 30, 2013

Charles Iheagwara, Ph.D., Managing Director
Unatek, Inc.

Table of Contents

1. Summary

Consistent with the scope and objectives of the State of Maryland legislative mandate, Unatek, Inc. conducted a Cyber security assessment of the State of Maryland State Board of Elections' (SBE) Online Voter Services (OVS) and underlying network system infrastructure from October 14 to December 30, 2013.

These objectives of the assessment were met through a multitude of vulnerability assessment and penetration tests. **The results of the assessment demonstrate that the Online Voter Services and the underlying network system infrastructure are resilient and that reasonable security controls have been put in place.** Nevertheless, the assessment provides the SBE with the opportunity to further the Cyber security and information assurance posture of the systems and to drive future decisions as to the direction of the emerging Cyber security requirements of the systems assessed.

1.1 Summary of Approach

The Unatek team conducted the assessment in accordance with the recommendations outlined in NIST SP 800 – 115: "Technical Guide to Information Security Testing and Assessment," in a manner that initially identified vulnerable system services and targets and then simulated a malicious attacker engaged in a targeted attack against the systems with the goals of identifying if a remote attacker could penetrate the system's defenses; and determining the impact of a security breach on the integrity of the OVS's order systems, the confidentiality of the OVS's customer information, and the internal infrastructure and availability of OVS's information systems.

- **Pre-planning**

The pre-planning for this assessment included a decision to engage the system with the specific intent to attack and determine if approved records stored in the Web application cookie and database were accessible and vulnerable to unauthorized "tampering" and, to determine if unauthorized access to the database were to occur or achieved could an attacker be able to insert new data records or alter existing data records. With this in mind, the Unatek team directed specific tools, designed to scan the Web application and the underlying database software in their current configurations on the servers, and report any settings that were deemed to be outside of, or contrary to "best security practices"; settings that should normally prevent tampering.

- **Assessment**

The assessment was conducted using a phased approach. Prior to conducting the vulnerability assessment tests, the Unatek engagement team reviewed all relevant documentations on OVS's design and architecture, and security posture to ensure that the design and architecture enforce the appropriate level of security as defined in the requirements. The review was extended to the systems security plan, textual documents, and other similar artifacts.

The remaining phases of the assessment were consolidated into two (2) major technical sub-grouping of tests.

In the first sub-grouping of test activities, the Unatek engagement team conducted a review of the security controls on the Voter Services Web Application including access control policies and procedures based on the Open Web Application Security Project (OWASP) framework, and the 2010 CWE/SANS Top 25 Most Dangerous Programming Errors (CWE/SANS) requirements. The security controls tests include automated vulnerability assessment and penetration tests to identify any weaknesses or vulnerabilities in the process steps of user logins and portal interactions that might permit the falsification of data or otherwise compromise the integrity of the process, and develop an audit program guide (APG) that will allow the SBE to audit the process on repeated occasions and accurately measure the integrity of the browsing and information access process.

In the second sub-grouping, the engagement team conducted a reconnaissance to uncover useful information that would aid the exploit of the OVS system infrastructure, and then examined the security of the host server that supports the OVS by performing focused vulnerability assessment exploits and penetration test against the server. The team used automated tools for the vulnerability assessment and audit of the security controls in the hosting server operating system and the database software that houses OVS information records.

During the penetration testing, the Unatek Cyber security specialist attempted to gain access that, under normal circumstances, would not be authorized. The testing was executed from the Unatek Cyber security center which is an external location to the OVS network system. Specifically, the Unatek Cyber security center was designed to emulate a scenario of an attacker that can assume a connection to the host server network and, having no specific knowledge of the host server network, affect penetration into the server to exploit vulnerabilities on the OVS.

The Unatek security specialist also examined the effectiveness of controls on the network router that establishes the boundary between the segment hosting the OVS computers and the rest of the corporate network. This was done first by using route discovery to the host server and then effecting some test examinations. The server was also tested for vulnerabilities but, in order to avoid any potential problems on the production system, prior notice was given the SBE/MVA

informing them of possible outage that could result from a "deep" exploration of the host server especially with the Denial of Service (DoS) attack test that was performed. After the network and operating system testing, the database was also examined using a tool specifically designed to test the internal database controls, this portion of the audit is considered an "application" controls review process and is intended to reveal any weaknesses or vulnerabilities in the logical configuration of the database processing and storage.

Finally, a qualitative risk assessment was conducted on the Ballot Duplication System (BDS). The BDS has a unique set of system architecture and is not a networked asset of the OVS system infrastructure.

Upon completion of the tests, the Unatek team analyzed the results of the test that provides the basis for the conclusions and recommendations.

1.2 Tools

The following tools were used in the assessment.

- Nessus
- Nexpose
- NMAP
- Visual Route
- IBM AppScan
- MetaSploit
- Wikto
- L0phtcrack
- Nessus
- Kali Linux Pentest Tool Suites
- Seige
- Burp Proxy
- w3af

2. Results

The test results were organized in the three (3) distinctive assessment areas:

1. Web Application Vulnerability Assessment
2. Penetration Testing; and
3. Database Assessment

Overall, the security assessment results did not reveal any vulnerability in the assessed systems that can either be internally or externally exploited or that are without effective compensating controls. Also, implemented security controls are effectively compensatory for minor lapses in the management of the OVS system technology.

3. Conclusion

The specific objectives of the Cyber security and information security assessment that were stated in the scope of work were met through the multitude of vulnerability assessment and penetration tests. The results and analysis of the assessments did not uncover any vulnerability that could be exploited to compromise the systems and it was determined that effective security controls have been implemented on the systems assessed.

Therefore, we conclude that a remote attacker would not be able to penetrate SBE's OVS's defenses.

4. Appendix 1: About Unatek, Inc.

Unatek Inc., the innovator in Information Technology solutions development and maintenance, and a leader in enterprise end-to-end IT security solutions, provides a complete suite of solutions and products that secure LAN and wireless networks and protect the extended mobile enterprise against all threats and attacks. Unatek provides customer focused consulting and technical services to both private sector businesses and public sector organizations. With industry experts, cutting-edge technologies, and time-tested processes, Unatek can anticipate, identify and resolve issues faster, more accurately and less expensively. Unatek's proven track records in the last seventeen years are a testimony of our ability to protect enterprises and their mobile users.

Incorporated on June 28, 1996 in the State of Maryland Unatek has over 17 years of dedicated support to the U.S. federal and State governments and commercial clients. Over the years Unatek has received numerous industry awards including the 2011 Maryland Incubator Company of the Year.

Past and current clients include:

- US Department of Homeland Security
- US Department of Labor
- US Department of Veterans Affairs
- US Department of Commerce
- US Smithsonian
- US Marine Corps
- DC government
- Maryland State Board of Elections
- Washington Metropolitan Area Transit Authority
- Metropolitan Washington Area Airports Authority
- Industrial Bank of Washington

Unatek is a current holder of GSA IT 70 Schedule award: GS-35F-0632T in addition to several other indefinite delivery/indefinite quantity (ID/IQ) contracts, and Blanket Purchase Agreements (BPAs).

- GSA IT 70 Schedule: GS-35F-0632T
- Department of Navy Seaport e
- US SBA 8a Method Sourcing
- Washington Suburban Sanitary Commission Blanket Purchase Agreement
- Metropolitan Water District of Southern California Master Contract: MA87002
- Washington Metropolitan Area Transit Authority Basic Ordering Agreement Contract
- Maryland CATS II Master Contract

5. Appendix 2: About the Principal Investigator Charles Iheagwara

Charles Iheagwara is the Managing Director of Unatek, Inc. He is also currently the Founder and CEO of IntrusionOnline Corporation. In his current role as Managing Director of Unatek, he oversees business development activities as well as pioneering the growth of the company in the global market.

Prior to his current positions, Charles worked in various consulting positions with the boutique management consulting firms of Grant Thornton and KPMG and the aerospace firm of Lockheed Martin. He was also previously employed by the financial services firm of Edgar Online.

Charles led Unatek to winning the 2011 Maryland Incubator Company of the Year award sponsored by The Maryland Technology Development Corporation (TEDCO), McGladrey, State of Maryland Department of Business & Economic Development (Maryland DBED) and Saul Ewing LLP. He is the recipient of the 2007 Maryland-India Business Roundtable's "Business Innovator of the Year" award.

Following an Invited Testimony, on July 25, 2011, Charles testified before the US Senate Committee on Small Business and Entrepreneurship on "The Role of Small Businesses in Strengthening Cyber Security Efforts in the United States."

Charles is an internationally renowned technology researcher with over 40 published scholarly publications. His work is widely quoted and he is a sought after speaker at several industry conferences. His academic background includes studies at MIT and Harvard and a Ph.D in Computer Science (Wales, UK), SM in Management (MIT) and several other advanced degrees.