SECURITY ASSESSMENT ACTION PLAN REPORT

For

San Bernardino County Employees Retirement Association (SBCERA)

December 5, 2014

151 Kalmus Drive, Suite L-4 • Costa Mesa, CA 92626 • www.AltiusIT.com

Table of Contents

I. Executive Summary

A. NETWORK SECURITY ASSESSMENT

During the period November 13, 2014 – November 15, 2014, Altius Information Technologies, Inc. (Altius IT) performed an on-site security assessment of SBCERA's information systems and related safeguards that ensure information security, confidentiality, and integrity.

A network security assessment is a method of evaluating the security of a computer system or network and related safeguards. Our review included a high level examination of various IT and physical network infrastructure controls related to equipment hardware, operating system software, network connectivity, facilities, and general business continuity practices.

B. PURPOSE AND SCOPE

The purpose and scope of the assessment included:

- A review and assessment of SBCERA's information security safeguards that protected against external and internal hacker penetration attacks.
- An assessment of the safeguards' appropriateness regarding SBCERA's size and complexity, the nature and scope of SBCERA's activities, and the sensitivity of information.
- A review of SBCERA's configurations to determine if the safeguards met or exceeded penetration information security program requirements.

C. APPROACH (WORK PERFORMED)

Altius IT evaluated SBCERA's internal information and physical security to determine if internal controls were sufficient and effective at protecting sensitive information. Our scope included a review of selected administrative, physical, and technical controls and safeguards. Our services did not include an assessment of SBCERA's policies, procedures, and related documentation.

II. Prioritized Findings and Recommendations

A. SUMMARY REPORT

This Security Assessment Action Plan Report is a summary document and our detailed findings are documented in the following separate reports that were previously delivered to SBCERA:

- Social Engineering Security Assessment Report – an evaluation of staff security education and awareness training.
- Security Assessment Report – an internal assessment of SBCERA's information and physical environment. Our report included exhibits to support our findings and recommendations.

This Report includes a prioritized summary of recommendations to enhance security and ensure information availability. We conducted the assessment in accordance with procedures we considered necessary to obtain sufficient and appropriate evidence to support our conclusions.

Based upon the information reviewed, discussions with staff, and tests performed by Altius IT, it is our opinion that SBCERA remains in the top 3% of systems audited. If SBCERA implements the recommendations included in this Report the effectiveness of the information security program will be enhanced.

Our recommendations should be aligned with business strategies to provide a strategic approach to reducing costs and generating more efficient operations. Intangible assets such as software and related compliance issues are an important part of asset management.

B. PRIORITIZED RECOMMENDATIONS

Altius IT's findings and recommendations are summarized in this Report and are grouped into three major categories:

- Major Non-Conformity (High Priority)
- Minor Non-Conformity (Medium Priority)
- Additional Observations (Low Priority)

Specific vulnerabilities are assigned to one of the above categories according to the severity of the specific issue, compensating controls that reduced or mitigated risk, the likelihood of the event, and the potential impact on the organization.

C. MAJOR NON-CONFORMITIES (HIGH PRIORITY)

Control	Report	Description
Acquisition, Development, and Maintenance	Information Security Assessment Report	*Cryptographic Controls (Section XIV.G.1).* Directories contained unencrypted sensitive data (e.g. names, social security numbers, etc.). Encrypt folders containing sensitive or confidential documents. Contact County ISD to determine options for encrypting sensitive e-mail communications. SBCERA is currently testing several potential solutions that will encrypt sensitive data when at rest. Solution should be in place 1st quarter of Fiscal Year 2016.
Acquisition, Development, and Maintenance	Information Security Assessment Report	*Vulnerability Management/Patch Management (Section XIV.G.2).* Many servers needed critical or high priority software updates or patches. Establish a formal patch management policy and procedures for servers, workstations, browsers, software applications, third party updates, etc. Updates should be tested before rolled out into production. Critical and high priority updates to be installed within 30 days of release. Microsoft released a large amount of patches two days prior to the network security audit. SBCERA had an informal policy of applying patches to its Test environment first, and then to the Production environment once validated. Patches were applied to Test within one week of release, and to Production within three weeks of release. Due to the timing and system requirements the patches had not yet been applied to either environment. SBCERA has formalized its patching policy, and shorted the time between initial release and when the patches are applied to the Test Environment.

D. MINOR NON-CONFORMITIES (MEDIUM PRIORITY)

Control	Report	Description
Organization	Information Security Assessment Report	*Security Audits (Section VIII.C).* Continue annual security assessments of technology systems, people, and processes. Scope to include an evaluation of administrative, physical, and technical safeguards and controls. SBCERA Information Services is audited each year as part of the larger Audit conducted by MGO. In addition a more detailed network and security audit is also conducted annually. No Change Required.
Human Resources	Information Security Assessment Report Social Engineering Security Assessment Report	*Termination or Change (Section X.E.1).* User management to state timeframe to keep account active (e.g. 2 months). IT places reminder on calendar. If IT does not receive a renewal request from manager within timeframe, the account is removed and archived. Current policy is to immediately deactivate all accounts upon termination, or resignation, unless otherwise requested by senior management. The policy has been updated to include a one month extension that can be requested by senior management, up to a total of three (3) months. *During Employment (Section X.E.2)*. Ensure initial and annual security training is provided to staff. Training to be appropriate for staff's roles and responsibilities. Ensure security reminders (e.g. newsletters, e-mails, posters, etc.) are used to remind staff of security risks. SBCERA Information Services has initiated formal staff security training.

D. MINOR NON-CONFORMITIES (MEDIUM PRIORITY)

Communications and Operations	Information Security Assessment Report	*Operations. (Section XII.O.1-4).* • Operations Procedures. Some procedures were documented but many remain undocumented. IT management to review critical business processes to ensure that appropriate and documented procedures are in place. SBCERA Information Services has reviewed and documented processes that were previously undocumented. • Monitoring and Review. Logs were reviewed manually. Consider a log analyzer that issues alerts upon predetermined events. Network is monitored by a logging application that generates email and text notifications. No Change Required. • Backups. Perform a study to determine compliance retention requirements. Retain year end backups to meet regulatory requirements. Design and implement a robust backup archiving solution that meets compliance retention requirements. Backups are generated daily, Weekly, Monthly, Quarterly, and Annually. Backup System currently meeting all retention requirements. No Change Required.

		• Media Handling (Portable Storage Devices). Portable storage devices to be managed from a central location. This ensures that selected workstations don't allow access to USB or CD-RW devices. Group Policy disables write access to CD-RW devices, and USB devices. Some exceptions apply depending on business processes. No Change Required.
Access Control	Information Security Assessment Report	*Access Controls (Section XIII.G.1-4).* • Access Management. Consider implementing controls that issue alerts and prevent unauthorized access/copying of sensitive information. System currently logs the access and copying of sensitive data. Alert notifications are now included as well. • Access Management. Passwords to expire no more than every 90 days. Passwords expire annually but are 15 characters in length to offset the longer expiration. Biometrics are also used where applicable. No Change Required. • Network Access Controls. Accounts to be locked after six (6) invalid logon attempts. Accounts currently lock after 5 attempts. No Change Required.

		• Network Access Controls. Ensure Virtual Private Network (VPN) users are terminated after 15 minutes of inactivity. VPN access terminates after 10 minutes on inactivity. No Change Required

E. Additional Observations (Low Priority)

Control	Report	Description
Asset Management	Information Security Assessment Report	*Licensing (Section IX).* Consider an asset inventory and management application that can assist in tracking purchased vs. installed licenses. SBCERA Information Services currently uses the asset inventory module of its Helpdesk software to track both physical assets as well as software assets, including licenses. No Change Required.
Physical and Environmental	Information Security Assessment Report	*Secure Areas (Section XI.C.1-2).* • Consider streaming a copy of video images off-site at the same time they are stored locally. Data center biometric entry logs are stored in data center. Consider off-site storage of logs. Video system is included in all backup scenarios. Though not streamed, data is retrievable. No Change Required. • Consider an audible alarm that sounds prior to the release of gas. Consider shutdown of power to data center prior to activating sprinklers. Consider automatic power down of systems prior to battery power exhausted. Audible alarm is sounded prior to gas dispersion (Cosco Fire Protection Verified). As part of the potential data center relocation, an automatic power shutdown prior to gas release is included. Servers currently power down automatically prior to batteries being exhausted.