ALEX PADILLA | SECRETARY OF STATE | STATE OF CALIFORNIA
OFFICE OF VOTING SYSTEMS TECHNOLOGY ASSESSMENT
1500 11th Street | Sacramento, CA 95814 | **Tel** 916.695.1680 | **Fax** 916.653.4620 | www.sos.ca.gov

ES&S Addendum Regression Testing Staff Report (EVS 5.2.1.0 CA)
Formerly (EVS 5.2.1.0)

Summary

The California Secretary of State's office began working with Elections Systems and Software (ES&S) to address multiple vulnerabilities identified during the Red Team (Security) Testing of the EVS 5.2.1.0 system. A path to mitigation was defined and several of the vulnerabilities mitigated in mid-September of 2017. From September 19 to September 22, 2017, California Secretary of State Staff, ES&S staff, and Freeman Craft and McGregor Group (FCMG) in addition to FCMG sub contractors applied security patches, applied updated scripts, and conducted functional regression testing of the system. Making such changes to the system submitted for certification, warrants a version number change. ES&S revised their application to reflect the version number change as EVS 5.2.1.0 CA, reflecting the security changes to the system, as now specific to the state of California.

Vulnerabilities Identified

The initial Red Team Security Report identified multiple vulnerabilities within the EVS 5.2.1.0 environment. There were three initial areas identified by the Secretary of State staff that required immediate mitigation. In addition, two additional vulnerabilities were addressed during the Regression Test, (1) a potential vulnerability with the Active Management Technology (AMT) framework within the Dell hardware components; and (2) the security seals used during the initial Red Team Test. Each is listed below along with the mitigation applied.

Vulnerability	**Mitigation**
Multiple Operating System Patches	The multiple operating systems patches were applied to each of the hardware components in the environment, two (2) servers Dell T630 and Dell T430, and four Dell OptiPlex 5040 workstation. The patches are current as of September 2017.
"Unquoted Service Path" on Servers and Clients	ES&S developed a Visual Basic script that was applied to the environment to address the "Unquoted Service Path" vulnerability. The first version was not adequate, and a second script was developed soon thereafter and applied, which successfully mitigated the issue.
Hardware Encryption	Full hardware encryption including Server, workstation, and auxiliary components such as

Vulnerability	Mitigation
	DS 200, DS 850, Express Vote will be addressed in future ES&S releases.
Dell AMT	Dell released a patch addressing the AMT vulnerability. That patch was applied to the Dell hardware components.
Security Seals	Several new security seals were tested. One "red and white" seal, appropriately left evidence of tampering, whereas the other seals provided, did not.

Regression Testing

Regression testing covered a General and Primary election, exercising functional scenario such as ballot configuration, tally, results reporting, ballot marking, and restoring election definitions. One fatal error occurred while attempting to finalize ballots for the Primary Election. It was determined the error occurred because of a coding error in the previously used election definition from the original functional test conducted earlier this year. There are specific steps to follow in such a scenario as demonstrated by the ES&S representative. While this is not a typical scenario for a jurisdiction, it should be noted in procedures if such an instance should occur, calling for a jurisdiction to restore an election like in the instance of a natural disaster, or any other disaster recovery scenario.

Conclusion

Two out of the three initially identified vulnerabilities were mitigated and the regression testing successfully completed. In addition, adequate security seals have been identified for use with the EVS 5.2.1.0 CA system. An additional vulnerability within the Dell hardware, possible AMT exploitation, was also mitigated using a vendor provided patch. The EVS 5.2.1.0 CA system was successfully tested during regression testing.