DEBRA BOWEN | SECRETARY OF STATE | STATE OF CALIFORNIA
1500 11th Street, 6th Floor | Sacramento, CA 95814 | Tel (916) 653-7244 | Fax (916) 653-4620 | www.sos.ca.gov

Security Plan For Top-To-Bottom Review

Maintaining the security of the equipment, source code and confidential documents submitted by voting system vendors and the independent testing authorities to the Secretary of State's office for the purpose of conducting the top-to-bottom review is of paramount importance.

To ensure all materials are securely stored and accessed, the Secretary of State's office has adopted a number of procedures that all Secretary of State and University of California personnel working on the top-to-bottom review are required to follow.

This overview of basic procedures is designed to provide the public and the voting system vendors who have entrusted the Secretary of State's office with their equipment, source code, and confidential documents with the assurance that the materials are being handled and stored in a highly secure fashion. However, this document does not include certain additional security procedures and processes that may be instituted as needed during the review, or that could pose a security risk if disclosed.

Requirements For Confidentiality

1) All review team members have been required to sign a statement that they agree to abide by a strict non-disclosure agreement (NDA) that precludes them from disclosing or discussing any proprietary or confidential information that they may obtain during the course of the review with any person not involved in the review.

Secure Facilities

1) The red team and accessibility testing will be conducted at the Secretary of State's office building, located at 1500 11th Street in Sacramento. The building has security guards onsite 24 hours per day, security cameras on all floors, and access to certain floors and areas are limited to secure key card access.

2) One room inside the Secretary of State's office building has been designated to house all of the equipment used in the top-to-bottom review and will serve as the facility for the red team phase of the review.

3) The room is secured and can only be accessed by personnel who have been issued electronic security badges. The entire room, including all of the voting system-related equipment, is under video surveillance 24 hours a day.

4) All of the voting system equipment is housed inside of a locked security cage for which only a limited number of Secretary of State personnel have keys.

5) The security cage houses a combination safe that contains all of the proprietary software and documents, including, but not limited to, source code, technical data packages, and reports from the independent testing authorities. The combination to this safe has only been given to a limited number of Secretary of State personnel.

6) A chain of custody log has been established and is maintained for each piece of equipment, source code and documentation that has been submitted to the Secretary of State's office by the voting machine vendors or the independent testing authorities. Any authorized person entering the secure room to access any piece of voting equipment, source code, or any other information stored inside the security cage or the combination safe must sign the security log for each piece of equipment, source code or documentation to be removed from the cage for examination and testing. Each security log entry must be verified by a second Secretary of State employee or University of California personnel working on the top-to-bottom review project. All equipment must be returned using the same procedure once the reviewer has finished using it for the day.

<u>How Materials Are Delivered To & Handled By Review Team Members Working Off-Site</u>

1) Copies of the source code and other electronic media are made and encrypted with key codes for use by the review team members. The key codes are known only to a limited number of Secretary of State personnel.

2) All source code and documentation delivered to a review team member for use and review outside of the Secretary of State's building is stored in a tamper evident serialized banker bag. The bag number is recorded and verified on a chain of custody log.

3) All shipping of bags to review team members is done using a process that allows the bags to be tracked throughout each stage of travel.

4) When the bags arrive at their final destination, the recipient has been instructed to store them in a combination safe until they open the tamper evident serialized banker bag.

5) After the bag has been opened, the reviewers are required to store the electronic media in a combination safe when not in use.

6) The recipient must contact the appropriate Secretary of State staff to obtain the encryption key code.

7) At the conclusion of the review, all source code, proprietary documents, and other confidential information is required to be returned to the Secretary of State's office or must be destroyed.