

ES&S SECURITY QUESTIONS FOR VENDOR

Revised 07/15/15

Answers provided as of 08/11/15

Karen Schutte:

- My question was whether or not the communication software and hardware is installed regardless, since we are not using it? If yes, can we deactivate it?

DS200 communications is performed using an optionally installed hardware module and requires a different DS200 software/firmware version to be installed as well. If both of these are not installed, then communications is not possible. In addition, the election definition must be configured with the correct option enabled, an additional security password defined, and the appropriate configuration data defined. If all of these are not configured and defined, then communications is not possible. In addition, the system does not allow communications during the scanning and tabulation processes. Communications is only enabled and possible for a very short window of time after polls are closed.

Arnie Urken:

- ES&S told us they hire an outside company to test security by trying to break into their system. I recall that they said that they employ the same company used by Lockheed Martin. What is the name of the company?

One of the initial security assessments of design and development of our voting systems was performed by an independent third party, Continuum Security Solutions. See reply below for ongoing testing activities.

- Is such “red team” testing done continuously or periodically? Does it include social engineering as well as attempts to break encryption systems? How would ES&S know if an encryption code had been broken?

The ES&S systems allow a county to canvass and audit the results on their own. Paper ballots are available to compare against the tabulated results at the scanner. Scanner reports are available to double-validate results reported at the central results reporting systems. Each and every release is submitted to a federally accredited voting systems laboratory, who will perform source code, security reviews and extensive testing.

- Does ES&S monitor the social and financial activities of engineers and others who might be vulnerable to outside manipulation?

ES&S performs a security background check and screening of each and every person as they are hired into the Company. ES&S does not monitor the ongoing social and financial activities of our personnel. ES&S maintains a strict separation of duties with regard to creation, build, and distribution of products and product versions. While engineers are able to change and enhance functionality for new products and versions, that is all they can do. Engineers cannot build production level products and cannot distribute products to the field. Different staff performs product builds, code is further reviewed by external parties, who then perform independent trusted builds of such code from the ground up, and products versions are then distributed by entirely separate parts of the organization.

ES&S and its Associates are strictly forbidden from engaging in politics, endorsing political candidates or parties, or making any political contributions for or on behalf of the Company. In addition, subject to applicable law, any Associates in the position of Vice President or above are strictly forbidden from directly or indirectly endorsing political candidates or parties, or making political contributions to any candidates, political parties, or election issues, or causes.

- How are updates handled to enhance security? What media and protocols are used to preserve code integrity?

Updates to enhance security or functionality are all internally tested by the ES&S Quality Assurance department and the ES&S Pre-Certification department. Then all such updates are reviewed by a federally accredited voting systems test laboratory (VSTL). The VSTL performs code reviews and then creates a trusted build using the reviewed code. Using the trusted build, the VSTL then performs rigorous functionality, load, stress, accuracy and security testing. All tests must be passed successfully before the release is provided to states and county customers, whereupon additional testing or evaluation may occur per each state's certification policies and practices.

- Does ES&S collect systems performance metrics that include aggregated statistics by voter type (mail ballot, precinct number)?

ES&S does not collect this type of information.

- If these types of data are collected, does ES&S destroy the data once users have completed an election? Are backups of election reports saved on disk or remotely that enable ES&S to compare elections over time, say Pima County school elections or Presidential elections?

This is not a service that ES&S performs. While the ES&S voting systems do create a wealth of log data, log files, and reports, such data is retained by customers and not typically sent to ES&S unless assistance in the review of the information is requested.

- Are users (voters or governments) protected by a statement of user rights?

ES&S provides an initial warranty and additional maintenance and support services that can be optionally purchased in support of our equipment.

- What happens if machine or system failure requires the County to rerun an election?

The ES&S systems are very reliable and extremely accurate. Customers can optionally purchase spare equipment that can be used and swapped in quickly if under a very rare circumstance that there is a failure of a specific machine in an election.

- Who pays?

We have not seen such an occurrence and do not expect this in the future.

- Does ES&S hold or offer insurance to deal with system failures?

ES&S does not offer insurance. ES&S is in the business of working with our customer base to conduct successful elections. We make things right for our customers.

- How does ES&S inform systems users about best practices, alerts, current challenges, and future security goals?

ES&S provides initial training and refresher training services. Best practices are documented and published in Product Advisory Notices (PANs). These PANs are provided to customers as necessary. ES&S also maintains a Customer Portal where product documentation and PANs can be accessed by our customers. ES&S also has Customer Service personnel who work with customers on site, as well as a Customer Service Help Desk that our customers can use to get advice and best practice information.

- How does ES&S integrate ideas for security into product/service development?

New ideas are continuously woven into product roadmaps and development plans. ES&S creates new version and upgrades in product releases periodically, but typically around once a year. These releases must go through

the federal and state certification processes before they would be released in a particular state. ES&S has on staff security trained and credentialed experts, who are involved in the design and development of the voting systems.

Tom Ryan:

- Is it possible for a central count computer user (county employee) to modify the election database manually?

No. It is not possible for a central count scanner operator to modify the election data on the system.

- If so, under what conditions? And is the action logged?

The central results reporting system, Election Results Manager (ERM), does have a facility to enter data manually. Access to this feature requires user authentication and only those users who have been given rights to this application can use it. This ERM manual entry facility has an integrated audit log built into it. All entries and changes using the ERM manual entry facility would be logged into the immutable, time stamped event log.

- What is the format of the election database? Is there any database file encryption? Other than the EMS, what software products would be capable of accessing the database?

The EVS system uses two databases. PostgreSQL is used for ElectionWare where the election definition is created. The Liant RM/COBOL ISAM database is used for ERM, where election results are stored. Both systems are locked down in hardened configurations so access to these databases outside of the ElectionWare and ERM applications is not possible.

Chris Cole:

- Can the memory card be programmed by the local people and if so can votes be switched?

Memory cards can be programmed by local elections staff. Votes cannot be switched. All data is only modifiable through the ES&S products, which all have integrated event audit logging facilities that cannot be worked around and are immutable.