Ohio Secretary of State

Ohio Secretary of State
DRE Security Assessment

Volume 1
Computerized Voting Systems
Security Assessment:
Summary of Findings and Recommendations

21 November 2003

InfoSENTRY Services, Inc.
www.infosentry.com
919.838.8570

RECOMMENDATION ES&S-09.1: ES&S should prepare, within the next 6-12 months, an enterprise-wide business continuity plan for all critical business functions involved with the design, development, manufacture, sales, and support of the products it has proposed for use in Ohio.

RECOMMENDATION ES&S-09.2: After establishing the business continuity plan, ES&S should carry out a formal desktop recovery exercise for its corporate headquarters and development staff.

FINDING ES&S-10: ES&S's offshore manufacturing facilities in Asia have achieved ISO-9000-family quality process certifications, but the firm's other facilities for software development and customer support have not received such quality certifications.

RECOMMENDATION ES&S-10.1: In addition to obtaining ISO-9000-family certifications for its software development processes and facilities, ES&S should undertake a project to achieve CMMI Level 2 status in order to improve its overall software maturity capabilities.

FINDING ES&S-11: ES&S is developing the ability to prepare a "voter verifiable paper audit trail" if Federal or State of Ohio standards require that functionality.

Summary of Findings and Recommendations for Hart InterCivic

FINDING Hart-01: Hart InterCivic maintains close contact with testing and certification authorities, clearing test exceptions and issues and moving new versions of products through certification process.

FINDING Hart-02: Hart InterCivic has considerable information system planning documentation and well-documented security planning processes, but they are not in a format that is consistent with integrated security planning documentation such as that detailed in Ohio's Information Security Framework or other international security planning documentation standards.

RECOMMENDATION Hart-02.1: Hart InterCivic should pull together its existing security management planning documentation into a format that is established in Ohio's Information Security Framework or another industry-recognized structures for information security management plans.

FINDING Hart-03: Hart InterCivic applies basic configuration management and change control techniques to its application development processes, but needs additional documentation and standardization of those processes.

RECOMMENDATION Hart-03.1: Hart InterCivic should devise and implement very strict, unified configuration management and change control procedures to all of its application development steps and assemble its documentation on those procedures into a cohesive, documented hardware, network, and software configuration management plan within the next 3 – 6 months.

FINDING Hart-04: Hart InterCivic maintains numerous information systems security policy and procedures documents, organized well according to requirements for submittal to ISO auditors and incorporation in an information system security plan.

FINDING Hart-05: Hart InterCivic has hired external consulting firms to prepare detailed network assessment and security risk assessments on its full information systems infrastructure and products.

FINDING Hart-06: Hart InterCivic has had no regular security audit of its critical business functions and information systems infrastructure.

RECOMMENDATION Hart-06.1: Hart InterCivic should have a Certified Information System Auditor or a professional certified as an information security auditor conduct an audit of its IS systems and operations within the next 6 – 12 months.

FINDING Hart-07: Hart InterCivic has provided information security training to its Operations and Information System (IS) Director, with more training scheduled in December.

FINDING Hart-08: Hart InterCivic has an on-going, documented information security awareness program and has provided an online security awareness course to all employees, including senior managers.

FINDING Hart-09: Hart InterCivic has recently developed a business continuity plan, but has tested only portions of that plan.

RECOMMENDATION Hart-09.1: After editing and revising its existing business continuity plan to add some missing details, Hart InterCivic should carry out a formal desktop recovery exercise covering at least its corporate headquarters and development staff.

FINDING Hart-10: Hart InterCivic and its contract-manufacturing partners have achieved ISO-9001 quality process certifications.

RECOMMENDATION Hart-10.1: In addition to its ISO-9000-family certifications for its software development processes and facilities, Hart InterCivic should undertake a project to achieve CMMI Level 2 status in order to improve its overall software maturity capabilities.

FINDING Hart-11: Hart InterCivic is in the planning stages for an ability to prepare a "voter verifiable paper audit trail" if Federal or State of Ohio standards require that functionality.

Summary of Findings and Recommendations for Sequoia Voting Systems

FINDING Sequoia-01: Sequoia maintains close contact with testing and Federal and state certification authorities, clearing test exceptions and issues and moving new versions of products through certification process.

FINDING Sequoia-02: Sequoia has considerable information system planning documentation and well-documented security planning processes as they move to comply with De LaRue security standards. However, the documentation is not in a format that is consistent with integrated security planning documentation such as that detailed in Ohio's Information Security Framework or other international security planning documentation standards.

RECOMMENDATION Sequoia-02.1: Sequoia should adopt the format that is established in Ohio's Information Security Framework or another industry-recognized structure for information security management plans as it moves to meet the parent firm's security guidelines.