REQUEST FOR INTERPRETATION BY THE NYS BOARD OF ELECTIONS

Requestor(s)	**Election Systems and Software, Inc.**

Request Date	**7/16/2010**

Requestor Contact Information *(Name, telephone, fax, mailing address, & email address)*	**Corey Skradski,** **11208 John Galt Blvd** **Omaha, NE 68137** **ph: 402-970-1100**

NYS Election Law, Guideline, or Other Issue to be Clarified *(cite specific reference)*	**VVSG 2005 Volume 1 Sections 7.8, 7.9, and C.2** “This software should be reviewed and approved by the Cryptographic Module Validation Program (CMVP). There may be cryptographic voting schemes where the cryptographic algorithms used are necessarily different from any algorithms that have approved CMVP implementations, thus CMVP approved software **should be used where feasible but is not required**.” [emphasis added] **New York State Regulation 6209.2.F.10(a)** “All cryptographic software in the voting system shall have been approved by the US Government’s Crypto Module Validation Program (CMVP) **as applicable**.” [emphasis added]

Statement of Ambiguity	As a general statement of understanding, NYSTEC has already stipulated that the referenced clauses allow for cryptographic usage that is not CMVP/CAVP certified. ES&S now brings forward three specific groups of code types to which it seeks a more direct ruling.

Facts Supporting Ambiguity	The ambiguity is now left in determination of what constitutes “as applicable” and “where feasible”.

Proposed Interpretation	The purpose of cryptography and its requirement is to ensure that data in the voting system is secure: that its Confidentiality, Integrity, and Availability are protected. CIA is a mantra in security circles. Protection in depth, providing security through multiple methods and layers is another. Ultimately, the protections afforded the data are dependent on the combination of all security layers and features, not just the cryptography, not just the access controls, not just the locks and seals, etc. **Group 1: Code within a system that is not utilized within the New York configuration** Code that falls into this classification exists in the system and is cited in the code review. However it is also clearly not executable in the system configuration deployed in New York. As such, this code should not be considered in the review and should be eliminated from the code review findings as

“de minimis”.

(Crypto Tab) Findings # 12,13,15,18,31,32,33,35,64,65,66,75,76,77,78, fall into this category.

Group 2: Code within a system that performs cryptography where cryptographic usage is not required

There are instances in the system where protection of data under cryptography is not required by the standards. In these instances, usage of cryptography affords added protection over non-use. In such cases, any level of cryptography is better than no cryptography.

Requiring these instances to meet the CMVP/CAVP certification requirement would in many cases force removal of the cryptographic protections since many of these are in portions where either the performance or the capability of the system component makes a CMVP/CAVP module not possible.

It would seem contrary to the ultimate goal of protecting the data to have these instances removed. As such, it would seem that use of cryptography that is not CMVP/CAVP certified should be allowed in these instances.

(Crypto Tab) Findings # 1,2,3,4,5,6,7,8,9,10,11,19,20,21,22,23,24,25,26,27,28,29,30,34,36,37,38,39,40,41,42,43,44,45,46, 47,48,49,50,51,52,53,54,55,56,57,58,59,60,61,62,63,67,68,86,87,88,89,90,93,94,95,96,97,98,99,100, 101,102,103,104,105,106,107,108,109,110; (Open-Security Tab) Finding #353 fall into this category.

Group 3: Validation of digital signature in locations other than where the system intends

There are locations in the system where digital signatures are generated and validated. There are other locations where the data is used but, since it has already been authenticated where required so re-authenticating is not necessary.

(Open-Security Tab) Findings # 306, 308,317 fall into this category.

NOTE: Attached with the RFI submission is a list of all the findings being referenced.

Please submit “Request for Interpretation” to:

NYS BOARD OF ELECTIONS
ELECTION OPERATIONS UNIT
ATTN: P. JORCZAK
40 STEUBEN ST
ALBANY, NY 12207

OR:

election_ops@elections.state.ny.us

NOTE: Interpretations by SBOE will be provided in a separate, attached, document.