Cryptography Requirements Gap Analysis

An overarching goal of the next VVSG is to have each requirement mapped to a principle and its associated guidelines. During the mapping activity for the Cryptography requirements, some requirements did not map well to the current list of principles and guidelines.

The requirements within the Cryptography section envision a specific architecture in order to protect election records, primarily based upon a specific technology. The NIST team is recommending that the end goal of cryptographically protecting election records remains, yet a specific method of doing so is not mandated. For instance, the use of Trusted Platform Modules (TPMs) should not be mandated. This drastically reduces the number of requirement within the cryptography section. Specifically, sections 5.1.2, 5.1.3, and 5.1.4 are removed.

Additionally, the requirements mandate the use of a FIPS 140-2 validated cryptographic module for all cryptography. Most software independent end-to-end (E2E) cryptographic voting systems use cryptographic algorithms or protocols that have not been standardized or approved by NIST. The cryptography underlying these voting systems is unlikely to go thru the FIPS 140-2 cryptographic module validation process, as these use non-standard cryptographic libraries. The Cybersecurity WG needs to discuss how to evaluate these protocols, and implementations of these protocols, within the EAC's voting system certification program.

Possible modifications for the cryptography related Principles and Guidelines include:

- The second guideline under Data Protection should be modified to state "**electronic records and other sensitive election artifacts**" instead of "electronic tabulation reports". The word "**cryptographically**" is also added to ensure this protection is not performed by a CRC or other insufficient method.

  *The source and integrity of **electronic records and other sensitive election artifacts** are **cryptographically** verifiable.*

  The term *electronic tabulation reports* is too specific. Instead we may want to require other critical or sensitive election artifacts produced by the machine to be digitally signed.

Due to the large changes in this section, there are no individual requirements listed below. The following topics are suggestions for future requirements:

- Protection of cryptographic keys
- Key management
- Key lifetime and freshness
- Cryptographic strength and keysize
- The use of FIPS 140-2 validated cryptographic modules

For more information about each requirement, please reference VVSG 2007 at:
http://collaborate.nist.gov/voting/pub/Voting/CyberSecurity/2007-VVSG.pdf