Data Encryption Testing Guidelines
For NYS Voting System Certification

The 2005 VVSG requires the use of encryption to protect the privacy and confidentiality of voting information when this data is transferred over a public network. Because NYS forbids the use of networks of any kind in our voting systems there is no VVSG or NYS requirement that clearly requires the use of encryption to provide data confidentiality. NYSTEC is in the process of determining a reasonable position on how to interpret the one requirement that we can lean on to require encryption in certain places within each voting system under test.

Part of our work on the security test case has been determining where encryption shall be required based on the following VVSG Vol. 1 Requirement 2.1.1a:

2.1.1 Security

System security is achieved through a combination of technical capabilities and sound administrative practices. To ensure security, all systems shall:

> *a. Provide security access controls that limit or detect access to critical system components to guard against loss of system integrity, availability, confidentiality, and accountability*

NYSTEC is interpreting the need to guard against the loss of confidentiality as meaning where encryption must be used. Digital signatures take care of integrity and to a degree accountability and the NYS Regulations are very clear on where digital signatures shall be used. Where confidentiality (preservation of privacy of data) is required however is less clear.

NYSTEC recommends the following guidelines to the ITA for where to test for the encryption of data.

Voting System Data	**Location**	**Encrypted** Shall = Required Should = Desired	**Justification**
Passwords (hashed), encryption keys and any other authentication data that must be kept private.	EMS, removable memory, scanners (everywhere)	Shall be	Security best practice, necessary for effective security controls.
Any data that if disclosed to an attacker could be used in a malicious manner to compromise voting system and thus the election. This could be vendor proprietary secrets that would have value in compromising the system or learning how to exploit a vulnerability. Any data that if disclosed would (by itself or when aggregated with other data) violate voter privacy and confidentiality of the ballot.	Removable media	Shall be	Removable media is not controlled like the scanners and EMS systems are, it is easy to copy and more difficult to control. Removable media is effectively the network in NYS. Prior to the use of scanner and EMS, software validation via hash check is used so inserted malicious code is detected. Vendors must encrypt sensitive data if they are relying on it as part of the security of the system.
Voted ballot images and individual ballot votes	Removable media	Shall be	The ability to steal a copy of all ballot images provides for a breach of voter privacy as voters who marked their ballots with identifying marks could be identified. Unprotected ballot images also helps to provide a vehicle for vote buying. These images would also be of significant value to corrupt politicians for determining where to contest elections and could also be used in the statistical analysis of voter choices.
Election summary results	Removable media	No	Results become public shortly after polls close anyhow, one time zone in NYS makes this risk too small to justify a shall.
Election audit logs	Removable media	Shall be	Because the election audit logs contain individual ballot votes and could be used in the statistical analysis of voter choices they must be encrypted. Corrupt politicians would pay for copies of this information and this information is not available publically.
All other voting system data	EMS and Scanner	Should be	EMS systems and scanners are protected by authentication controls, physical security and most importantly by integrity controls including software validation via hash checks as well as the use of digital signatures. These protections when used provide sufficient protection of voting data.