

ATTACHMENT R

BIDDER'S SECURITY PROPOSAL

Bidder should describe how their proposed solution will comply with any applicable policies, standards, laws and rules, including but not limited to:

- All policies and standards defined in the New York State ITS security policies and standards (<http://its.ny.gov/eiso/policies/security>), including, but not limited to:
 - NYS-P10-006 – Identity Assurance Policy,
 - NYS-S13-001 – Secure System Development Life Cycle Standard,
 - NYS-S13-002 – Secure Coding Standard (if applicable),
 - NYS-S13-004 – Identity Assurance Standard,
 - NYS-S14-003 – Information Security Controls Standard,
 - NYS-S14-005 – Security Logging Standard,
 - NYS-S14-007 – Encryption Standard,
 - NYS-S14-013 – Account Management / Access Control Standard
 - NYS-S15-001 – Patch Management Standard (if applicable) and
 - NYS-S15-002 – Vulnerability Scanning Standard.

The proposal shall address the following:

1. Confidentiality, Integrity and Availability of data at rest and in motion, including how the NSY DOH requirements related to data and system security will be addressed.
2. Network security, including server management; network configuration; system and application vulnerability prevention, detection and management; secure data transmission but in the application and in support of the system; account management; incident handling; and logging and auditing of security events.
3. Application security, including application use auditing; secure coding practices and overall NYS Secure System Development Lifecycle (SSDLC) documentation and management, including any processes and tools used in the process.

