State of New Jersey
Office of Information Technology
P.O. Box 212
Trenton, New Jersey 08625-0212

Chris Christie
Governor

E. Steven Emmanuel
Chief Information/Technology Officer

File Transfer Guide
As of April 10, 2012

Extranet Plan

The contractor shall provide and maintain two (2) extranet communication links into the State of New Jersey. One of these links will be active and one will be a "hot" spare. These links shall terminate as follows:

- Link 1 – Ethernet speed or greater communication circuit shall be established from the contractor's data or communication center to the State of New Jersey's Primary Data Center at OIT HUB, 1 Schwarzkopf Drive, West Trenton, NJ to operate as the primary data path. This data circuit shall provide the primary path and should terminate on the State of New Jersey side into the contractor-owned and maintained equipment, which in turn would provide an Ethernet connection to the State's Extranet Partner access point at OIT Hub (firewall).
- Link 2 – Ethernet speed or greater communication circuit shall be established from the contractor's data or telecommunication center to the State of New Jersey's Hamilton Data Center at OIT OARS - 1200 Negron Dr. Hamilton Twp, NJ or SAC Data Center - River Road PO Box 7068 W. Trenton, NJ 08628 to operate as the secondary data path. This data circuit will provide a secondary backup path and should terminate on the State of New Jersey side into the contractor-owned and maintained equipment, which in turn would provide an Ethernet connection to the State's Extranet access point at OARS (firewall) or SAC (firewall).

The awarded contractor must work with the sponsoring agency and OIT to establish an Extranet Partner relationship. This would require completion of an Extranet Partner agreement and documentation; reference the State of New Jersey's extranet policy 09-11-NJOIT (http://nj.gov/it/ps/security). In addition, the contractor staff must work with OIT network staff to establish the appropriate routing protocols based on the system requirements and OIT security staff to establish appropriate firewall rule sets to accomplish necessary business data flow.

The communication links can connect to a MPLS cloud or IPSEC tunnel over the Internet based upon the connectivity requirements and cost constraints. Once the communication links are established and testing is completed, the OIT Hub will be the primary link to the contractor.

Transmission of Files

The State of New Jersey supports multiple methods for data transfers internally within the Garden State Network or external to an extranet or business partner. The transmission of all files between the contractor and the State system must be transferred securely using the State file transfer methodology. The State will work with the contractor in the implementation of the file transfer process. The secure file transfer must meet the state and federal security guidelines and standards.

The State of New Jersey provides both asynchronous and synchronous file transfer methodologies.

Synchronous:

1) Connect:Direct Secure + is a supported option for file exchange with the State of New Jersey IBM mainframe.

2) FTPS over SSL (Explicit – port 21) is a supported option for file exchange for connections originating from the State of New Jersey IBM Mainframe. Must support RFC2228.

3) SFTP (FTP over SSHv2 or greater) is a supported option for file exchange with State of New Jersey distributed servers (non-IBM Mainframe).

Asynchronous:

1) The State of New Jersey's DataMotion or Tumbleweed are a supported option for non-automated or "ad-hoc" file exchange with State of New Jersey. A client license is required.

2) The State of New Jersey's DataMotion-DataBridge is a supported option for automated file exchange with the State of New Jersey.

The proposed high level process flow is as follows:

Flow diagram

The contractor will be required to test the file transfer with the State system on all file transfers prior to full implementation.

During the life of the contract, the State may revise or change the file transfer method and/or format for the transmission of files to accommodate real time processing, and use case specific information and the contractor shall be required to conform to all requirements.

Reference:

NIST Special Publication 800-53A - Guide for Assessing the Security Controls in Federal Information Systems and Organizations (http://csrc.nist.gov/publications/nistpubs/800-53A-rev1/sp800-53A-rev1-final.pdf)

NIST Special Publication 800-47 - Security Guide for Interconnecting Information Technology Systems (http://csrc.nist.gov/publications/nistpubs/800-47/sp800-47.pdf)