**EXHIBIT A**

# State of New Jersey
# Office of Information Technology

## File Transfer Guide

## Extranet Plan

Extranet Use Cases

- The need arises that an external 3rd party needs to initiate file transfers to a GSN Department or Agency.
- Information Exchange between external parties needs to be secured or routed over a private connection.
- Vendors, 3rd Parties or other External parties want to build a private connection to an entity on the GSN, while avoiding the uncertainty of using the Internet as a medium. Utilizing the GSN Extranet service via private line allows bandwidth to be guaranteed and eliminates the fluctuations of speed and latency that would otherwise be impacted on the Internet.

Extranet Options

The communication links between the State of New Jersey and the contractor can be through a dedicated circuit or IPSEC tunnel over the Internet based upon the connectivity requirements and cost constraints.

The contractor must work with the sponsoring agency and OIT to establish an Extranet Partner relationship. The State of New Jersey and the Contractor will be required to follow the State's Extranet Policy and Procedure, and complete the application form, MOU, operational form and security controls assessment checklist.

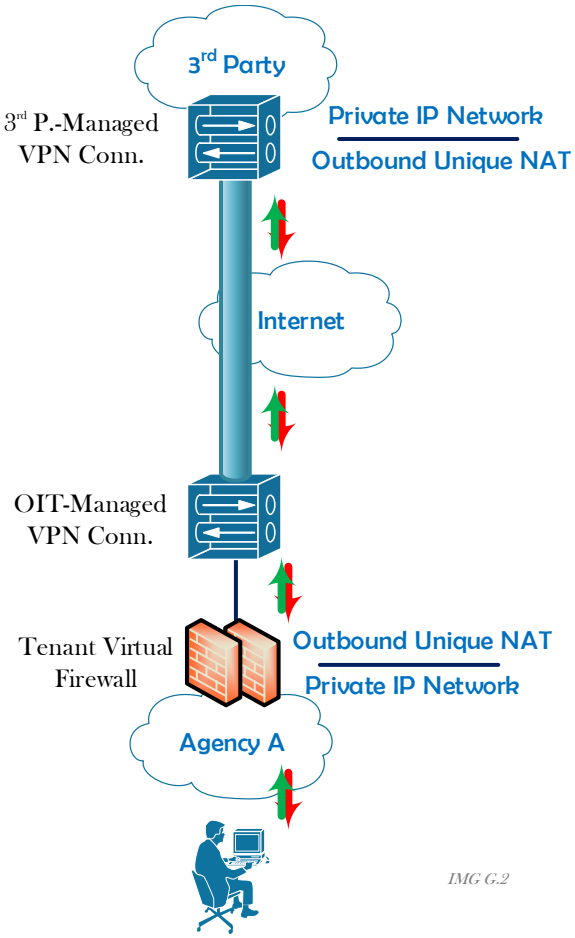
The State agency and external 3rd Party must agree on the Extranet service level they will be utilizing for the connection, the cost of the connection and who will be paying for the agreed upon services.

The State currently supports the following four service levels:

- Extranet Bronze – Single IPSEC Tunnel over the Internet.
- Extranet Silver – Single dedicated circuit from a telecommunications carrier.
- Extranet Gold – Dual IPSEC Tunnel over the Internet from our HUB and Hamilton Data Centers.
- Extranet Platinum – Dual dedicated circuits from a telecommunications carrier from our HUB and Hamilton Data Centers.

**EXHIBIT A**

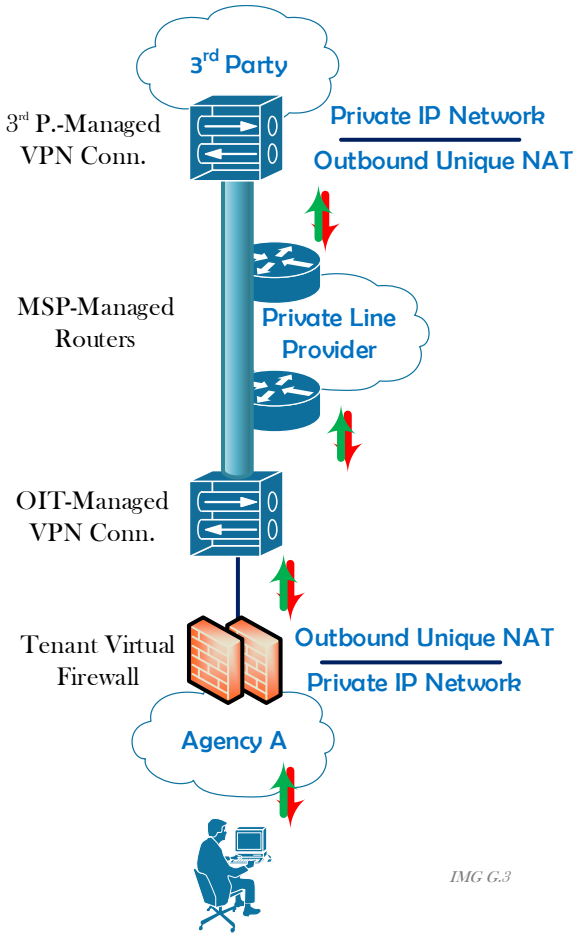
# Extranet Topology and Technologies




## Extranet Specifics and Topology (Bronze)

- Various IPSec configuration parameters are supported and should at a minimum meet the recommended values as defined by NJOIT's GSN Technical Architects.
- Bandwidth over the Internet is not guaranteed.
- Internet instability may cause disruption of this tunnel, therefore this Extranet model is considered best effort.

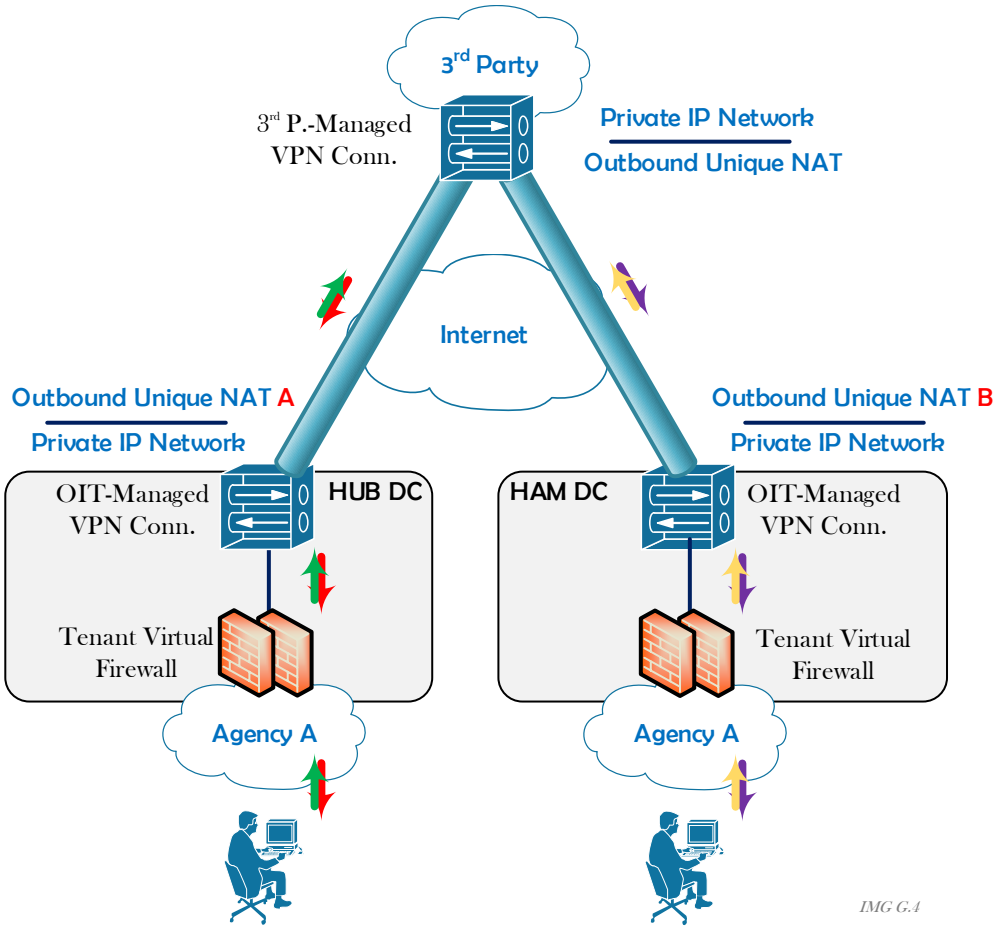
**EXHIBIT A**




## Extranet Specifics and Topology (Silver)

- All management and administration of the physical connectivity to the 3rd party carrier router is handled by the OIT Data Center Infrastructure Group and all equipment meet the Data Center's Electrical standards. (The Carrier Router and circuit must terminate at the West Trenton or Hamilton Data Centers.)
- Management of the Private Line Provider is the responsibility of the vendor or the Agency requesting service.
- Bandwidth over Private Circuits is typically guaranteed (depending on what the 3rd Party Vendor has requested from the Carrier)
- Incidents determined to be fault of the 3rd Party or Private Line Provider are the responsibility of the Agency or 3rd Party to remediate.

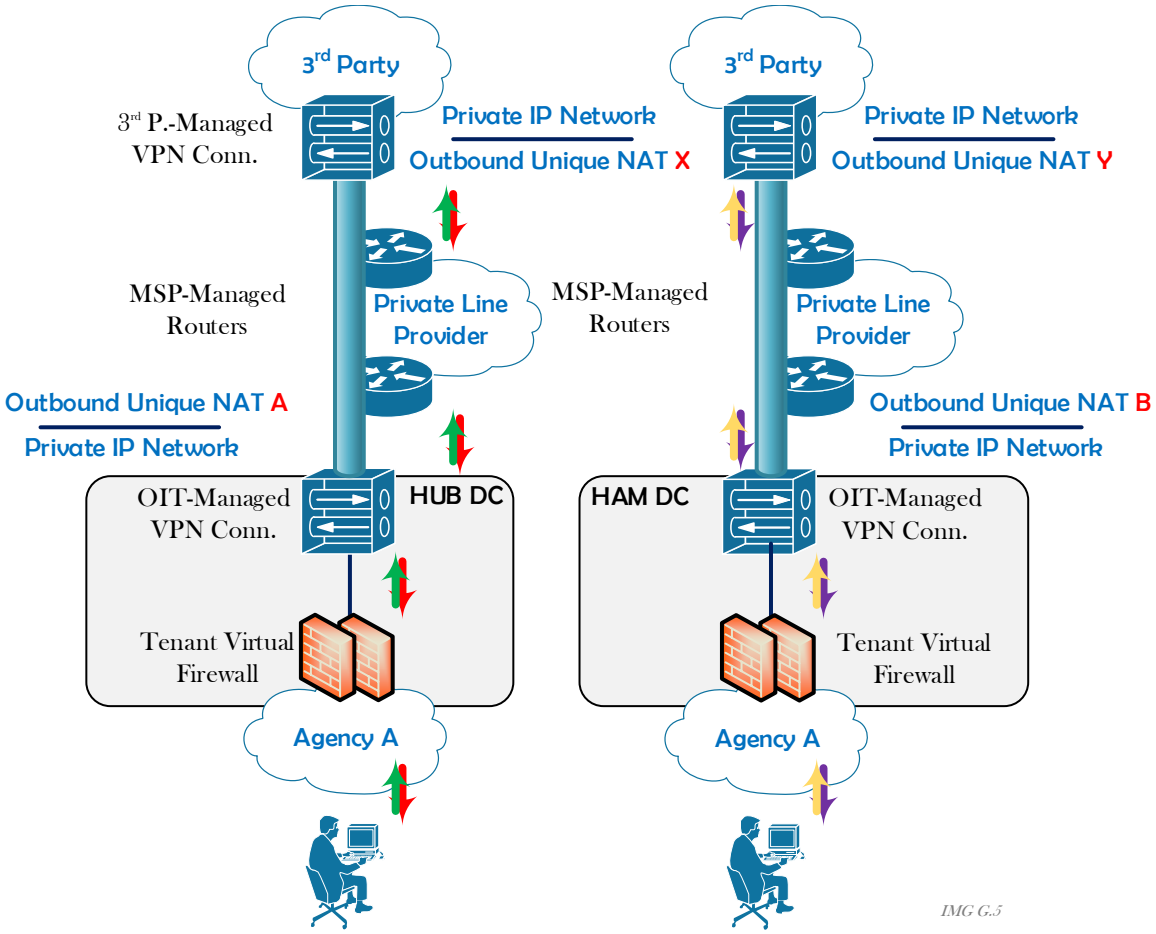
**EXHIBIT A**




## Extranet Specifics and Topology (Gold)

- Similar attributes and requirements to the Extranet Bronze Service, only dual-homed
- Each Data Center connection acts independently, and provides Unique NAT addresses at each connection point
- Applications can be configured to use one or both paths (depending upon the configuration of the App and the DNS resolution of IP Addresses for each tunnel.
- Traffic across each tunnel for similar IP Advertisements are treated as Active/Standby to avoid asymmetric traffic flow (traffic cannot leave through one VPN and return through the other – this traffic will be dropped).

**EXHIBIT A**




## Extranet Specifics and Topology (Platinum)

- Similar attributes and requirements to the Extranet Silver Services, only dual-homed with dual private carriers
- Each Data Center connection acts independently, and provides Unique NAT addresses at each connection point
- Applications can be configured to use one or both paths (depending upon the configuration of the App and the DNS resolution of IP Addresses for each tunnel.
- Traffic across each tunnel for similar IP Advertisements are treated as Active/Standby to avoid asymmetric traffic flow (traffic cannot leave through one VPN and return through the other – this traffic will be dropped).

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