

Enterprise IT Shared Services Service Level Agreement



Customer Networking Solutions Details

(Revision Date: September 15, 2010)

**DOCUMENT CONTROL
REVISION HISTORY**

<i>DATE</i>	<i>DESCRIPTION</i>
9.15.10	INITIAL RELEASE

TABLE OF CONTENTS

CUSTOMER NETWORKING SOLUTIONS

INTRODUCTION.....	4
SERVICE DETAILS.....	5
Network Operating Services (NOS)	5
Internet Access.....	7
Data Communications	8
24x7x365 LAN/WAN Maintenance & Support	12
SSLVPN (Secure Socket Layer Virtual Private Network).....	12
Workstation Configuration Management & Support.....	13
Endpoint Security.....	15
Transaction Terminal Security Systems.....	17
SharePoint.....	17
ORDER PROCESS.....	18
ROLES AND RESPONSIBILITIES	19
SUPPORT	22
COMMUNICATION	26
LEGAL AND SECURITY ISSUES	28
HOW RATES ARE CALCULATED	29
RESOURCES	35
CONTACT US	36

INTRODUCTION

The purpose of this document is to provide detailed Service Level Agreement (SLA) information about the Customer Networking Solutions.

Customer Networking Solutions offers a composite of centralized, managed networking services to provide safe and secure connections to the NYeNet, CIO/OFT Statewide Data Centers and state agencies. Customers will work with an experienced team who are recipients of the Best of New York award for “Best Practice in IT Infrastructure Management.”

This document is part of a set of SLA documents, and part of a group of documents and web pages that contain information about the Customer Networking Solutions. The Resources Section of this document provides links to CNS resources.

SERVICE DETAILS

CIO/OFT can manage your local and wide area network and provides a comprehensive suite of services.

NETWORK OPERATING SERVICES (NOS)

This service provides authentication services for log in and resource access, authentication for remote access, file and print services, and provisioning.

This service is available 24x7x365. The support for this service is available during Standard Business Hours unless otherwise negotiated. To extend support for this service please refer to the service description for 24x7x365 LAN/WAN Maintenance & Support for details.

Administrative Model

The administrative model service provides design, establishment, and maintenance of network organizational structures for the purpose of administration, security and access control for storage of user data, administration of users and administration of computers.

CIO/OFT will:

- Design and provision organizational structures, upon receipt of a service request this includes:
 - a. Determining organizational structure size
 - b. Investigating network WAN capabilities
 - c. Applying security to objects
- Delegate provisioning capabilities of the organizational structure to an approved individual or group.
- Evaluate the need for planning, moving and consolidating of organizational structures when warranted.
- Plan and decommission organizational structures when appropriate
- Monitor, troubleshoot and proactively manage organizational structures for health and performance.

File and Print Component

File and print provides users with home directory shares, disk space for data shares, print shares, and disk space for application shares.

CIO/OFT will:

- Actively monitor disk infrastructure for impending failures
- Work with Agency and system administrators to identify storage related performance issues and resolve or recommend solutions
- Resolve problems and coordinate problem resolution with vendors when appropriate
- Track and review disk resource utilization and performance to make resources available to meet Agency requirements
- Configure and expand disk resources as required
- Design cost effective disk resources based on best practices for security, performance, availability and scalability
- Provide user home directory shares up to a maximum of 100MB per user
- Upon the receipt of a Service Request, add or remove disks resources space for servers.
- Migrate home directories to appropriate servers as needed

Provisioning

CIO/OFT provides a process to create and maintain valid user accounts, e-mail objects, file objects, and application authorization for appropriate users in the NOS Directory using an internally developed application called Webstar. Webstar is used to provide full function provisioning while limiting administrators' scope of operations to those areas they are responsible for. Webstar is available to the Agency administrators through a web interface and allows an Agency administrator a single point of access to the Users attributes. The service is a delegated administration model where the activities associated with it are performed in various units throughout the State.

CIO/OFT will:

- Provide and maintain a web based provisioning tool
- Maintain documentation relating to the use of the provisioning tool
- Work with delegated administrators to resolve problems with the tool and/or its use upon the receipt of a trouble ticket or Service Request
- Evaluate feedback from users on enhancements to the provisioning tool and makes changes as warranted
- Evaluate requests to create delegated administrator accounts and creates them when warranted
- Establish additional application access controls
- Maintain access control lists and permissions on a regular basis

INTERNET ACCESS

This service is available 24x7x365. The support for this service is available during Standard Business Hours unless otherwise negotiated. Please refer to the service description for 24x7x365 LAN/WAN Maintenance & Support for details on extending support for this service.

Internet Access provides safe, content controlled, Internet web access to authorized users through the customer network. This service consists of three components:

Internet Proxy Services

The Internet Proxy component of this service reduces security risks by preventing internal network addresses from being exposed to the Internet and provides the means to limit Internet access to authorized users. Proxy services also improve Internet browsing performance by caching frequently used web pages.

Authorization is based upon NOS Directory groups consistent with the Active Directory. This component integrates with Microsoft's Internet Security and Acceleration Server application (ISA) to authenticate the user.

Content Filtering

The Content Filtering component of this service applies content controls to Internet web-browsing activities. These controls provide a layer of security to customer computers by providing protection against both malicious content and inappropriate web usage such as malicious file downloads, adult content and criminal activity. Filtering additionally reduces legal risks and productivity losses associated with uncontrolled Internet access from the worksite.

Controls can also be used to manage the use of Internet bandwidth by blocking access to non-work-related sites.

Content Filtering is handled through two methods:

- a. "White-lists," to allow access to a strictly defined group of websites
- b. Filtering software, to provide wider access.

Web Anti-Virus and Anti-Spyware

Following the best practice of layered defenses, filtering tools are placed between Proxy servers and the Internet to provide a first line of defense against Internet threats. These security tools scan HTTP and FTP web traffic for hostile code and malicious content, offering an additional layer of security for Internet users.

Internet Access Options

Customer options are based on the level of access requested by the customer Agency for each individual user when the account is created. Agencies have the ability, through the WEBSTAR provisioning tool, to change the group membership and thereby permit or deny Internet access. All Internet usage is billed equally, and is determined by user membership in any of the following Active Directory groups:

1. ProxyBlock: No access (no charge).
2. Proxy Restricted: In this category, Internet access is restricted to an approved list (historically referred to as the GOER list) of Internet sites to support Centraport and a limited number of approved work-related sites.
3. ProxyLimited: This category allows Internet access limited to an approved list of categories (e.g. .edu, .gov, etc.) allowed through content filtering software. This provides greater access than the Proxy Restricted group, but is more limited than the Full Access group.
4. ProxyFull: This category allows full Internet access. Content filtering software is used to block access to categories such as malicious, illegal, and pornographic websites.

DATA COMMUNICATIONS

This service comprises a number of infrastructure, firewall, and connectivity services.

This service is available 24x7x365. The support for this service is available during Standard Business Hours unless otherwise negotiated. For details on extending support for this service, please refer to the service description for 24x7x365 LAN/WAN Maintenance & Support.

Remote-Site Local Area Networking (LAN)

This service provides interconnection of remote offices to the Agency's core site and State Data Centers. This is an IP only network solution, which meets NYeNET security standards. The design provides appropriately sized NYeNET WAN/E-port circuits, remote site router/E-port equipment, and Data Center connectivity via a secure VPN tunnel over E-port. Customer Networking Solutions will consult with the Agency concerning their functional requirements and develop the bandwidth requirements for an optimal WAN solution. CNS will procure, schedule and install all equipment that is part of the data communications configuration.

This service also provides interconnection of IP network devices at the remote site. Standard equipment will be either 24 port or 48 port 10/100 Ethernet switches, depending upon site sizing requirements. Upon receipt of a Service Request, Customer Networking Solutions will

perform a site survey with the customer representative at the site to determine all details, such as inter-closet cabling and power requirements. Agencies are responsible for the cost of site cabling, power for equipment, and other site prep identified in the survey.

CIO/OFT will:

- Provide all LAN data communication equipment and maintenance
- Troubleshoot switches and router problems when necessary

Remote networking provides the following devices:

- Layer 2 devices – Ethernet switches that workstations connect directly to
- Small/Medium Layer 3 devices – Routing/ VPN tunnel devices that connect the local area network (LAN) to the wide area network (WAN)
- Large Layer 3 devices – Routing/VPN tunnel/LAN aggregation devices that consolidate the LAN segments at remote sites and connect them to the WAN

Wide Area Networking (WAN)

Data Communications provides WAN services to connect remote sites to the customer core.

CIO/OFT will:

- Monitor bandwidth use and network layer congestion on an ongoing basis utilizing network management equipment
- Proactively monitor the network for potential problems
- Analyze the use, cause, and remediation of up/down alerts
- Diagnose primary alerts (loss of connectivity)
- Work with vendors on problem resolution and completes trouble tickets with CCC Level 1 support (Circuit Calls)
- Provide access to bandwidth use reports to check for trouble on circuits upon request from IT organizations.
- Provide support for infrastructure problems that have been diagnosed as hardware or software manufacturer defects residing on the Network architecture, including, but not limited to routers, switches, VPN devices, and other network devices as required by the design.
- Procure, schedule, install, and maintain all equipment that is part of the data communications configuration.

Core Routing

Core Routing provides the ability for remote sites to communicate with each other, as well as with servers located at the core location. It also provides the network path to applications in the State Data Center, as well as connections to other state and local governments, Agency business partners and the Internet.

Firewall Services

CIO/OFT provides managed firewall services. This service provides a secure, high-speed connection to the Internet for client access to Internet resources from the core site of the customer network, proper segregation between the customer network and remote sites, which have been integrated with customer network and segregation and protection of resources within the customer network, which require such. Firewall services protect from intrusions while still allowing users to access the Internet and other networks using a combination of hardware, software, and access control policies by allowing proper inbound access to Agency applications and resources. This service also provides secure high-speed connections and protection for devices inside the network to limit communication between and among devices, which ensures proper device-to-device communication over specified and approved ports.

CIO/OFT will:

- Provide an initial security needs assessment
- Provide firewall hardware and software and maintains and/or replaces it as needed
- Install and configure firewalls
- Evaluate requests for changes and implementation of changes if deemed appropriate
- Manage firewalls daily and maintains rules to permit the flow of acceptable traffic
- Support firewalls and set up and monitor operational alerts

(Note: Proxy services, content filtering and anti-virus protection are described in the Internet Services section of this document and would be integrated with this service.)

DNS and DHCP Services

CIO/OFT provides Domain Name Services (DNS), across all sites in the customer network, allowing client workstations to locate applications servers without local configurations on the workstations. Statewide DNS will be provided to Agencies for access to their applications on NYeNET. Internet Zones will be maintained for an Agency's Internet accessible applications.

CIO/OFT also provides Dynamic Host Control Protocol (DHCP) services, which involves the provisioning of IP address assignments for workstations, and allows for central management of IP addresses. This prevents duplication of IP addresses, which prevents workstations from operating, and reduces Agency effort in maintaining workstations.

CIO/OFT will:

- Provide DNS service for hostname resolution for hosts on the NYeNET
- Evaluate and assist in the deployment of DNS servers for the NYeNET
- Manage the DNS databases on DNS servers to ensure integrity of data
- Interface and manage Internet DNS entries for those hosts in the CIO/OFT assigned zones

- Work with other governmental organizations to transfer DNS zones between networks
- Receive, evaluate, and process requests for DNS entries for both the NYeNET and the Internet

CIO/OFT will provide DHCP service to identified workstations for customer networks within prescribed IP address ranges. With this service CIO/OFT will:

- Manage IP address pools to ensure a sufficient number of IP addresses
- Manage DHCP servers to ensure that DHCP services are readily available
- Distribute IP addresses dynamically based on ranges identified for a particular network
- Manage leases of IP addresses, which will resolve conflicts in DHCP IP addresses

Network Design Services

Upon receipt of a Service Request for networking equipment, CIO/OFT will provide network design, implementation and support services for Wide Area Networks to Agencies. CIO/OFT will perform a Site Survey and conduct steps necessary to order circuits and equipment, add switches/circuits/ routers, and manage circuits. Upon completion of the Site Survey and the scope of work definition, it will be turned over to the CIO/OFT Implementation group.

Agency Partner Access Including Onenetnys

This service provides controlled access to applications from Agency business partner networks such as a vendor or Federal/State/Local partner Agency. Various techniques are used, based on the access and security requirements.

CIO/OFT will:

- Provide network access to outside entities that function as Partners to the Agency (e.g. a vendor that provides fiscal functions, or a non-profit that provides program functions for the Agency). Partners can be Federal/State/Local Agencies or vendors.
- Provide partner circuits that connect to the network and its services. The partner circuit may connect a Partner network with the Agency network. The circuit may be provided by the Partner or provided by CIO/OFT and billed back, depending on the situation.
- Require participation of Partner staff during the design and implementation phases in order to assure that the security objective of both parties have been met. CIO/OFT will consult with the Agency about their requirements for access with the Partner and will develop a strategy that addresses the needs of the Parties.
- Provide controlled access for a variety of services, such as applications housed in the State Data Center, or Agency applications or services that reside elsewhere on the network as required.
- Design, test, and develop technology solutions used to meet the various connectivity needs.

- Select technologies to provide service, and align the access with the needs and availability (e-port, SSLVPN, etc.).
- Ensure that the connectivity is protected by authorization ensuring allowed access is available, but security is not compromised.
- Support and maintain the centralized networking hardware and software devices needed to control the access (e.g. firewall).
- Require all interconnects be between partner Agencies and the core network at the customer core or at the State Data Center.

24x7x365 LAN/WAN MAINTENANCE & SUPPORT

This service extends prime shift maintenance and support to 24x7x365 for Data Communications services described within this document and raises all CIO/OFT maintained equipment at the site to 24x7x365 coverage. Off-hour coverage is initiated by a call to the CCC, with Level II and III data communications technical support on call. Off-hours support is provided for Customer Networking Solutions products and services only. The cost for this service is in addition to the regular rate, and will be quoted on a site-by-site basis.

SSLVPN (SECURE SOCKET LAYER VIRTUAL PRIVATE NETWORK)

This service provides application level access from workstations outside the network without the security risk of a direct network layer connection.

This service is available 24x7x365. The support for this service is available during Standard Business Hours unless otherwise negotiated. Please refer to the service description for 24x7x365 LAN/WAN Maintenance & Support for details on extending support for this service.

SSLVPN facilitates application access over the Internet or NYeNET, via a user's browser. This service allows users to access a specific application program (or group of application programs) through a Secure Socket Layer (SSL) session. Access to applications is defined by the rights assigned to each user's user-id. Access to any other applications and all network resources is blocked at the core SSLVPN switch. The PC does not need to be administered by CIO/OFT. Once configured, the administration of access is delegated to the customer Agency who manages group access. End users need access to a pre-established URL using SSL (port 443).

This functionality is similar to that of an SSL enabled reverse proxy web server. The SSLVPN appliance creates an SSL encrypted session between the user's web browser and the appliance. The appliance also creates a separate session with the application server and forwards data requests from the user session to the application session.

WORKSTATION CONFIGURATION MANAGEMENT & SUPPORT

This service is available 24x7x365. The support for this service is available during Standard Business Hours unless otherwise negotiated. Please refer to the service description for 24x7x365 LAN/WAN Maintenance & Support for details on extending support for this service.

The CIO/OFT Workstation Configuration Management & Support service provides comprehensive management of workstations throughout their lifecycle. This service provides pre-deployment and deployment activities, creation & maintenance of the base workstation image, configuration management for deployed workstations, and telephone-based technical support.

Onelimage

OnelimageNYS is a new product that reinvents the concept of workstation imaging & deployment for CIO/OFT customers. Instead of creating custom images for each workstation model or customer program area, OnelimageNYS provides a single base image that can support virtually any hardware or program.

Additionally, OnelimageNYS is deployed via the network, and is regularly updated with application, security and anti-virus updates.

For new workstation or laptop rollouts, OnelimageNYS can be certified to run on new hardware in approximately one week. For technicians working on PCs, OnelimageNYS's network based install process reduces re-imaging time by 80% to about an hour.

Software Distribution

This offering delivers software and configuration changes to deployed workstations. Scalable systems deliver software to thousands of computers with little or no impact to WAN bandwidth utilization or customer operations.

Software Distributions are conducted with close cooperation from customer Agency staff. For Windows Security Updates, Agency IT staff test updates against critical applications before updates are released to production equipment. For other software updates, customer software developers or IT staff partner with CIO/OFT staff to create and test customized software packages.

Site Survey

CIO/OFT evaluates the physical location & infrastructure to develop detailed office or site-specific documentation to be used in all phases of workstation deployment. Depending on project requirements, a survey may examine (but is not limited to) site security, device inventory, electrical capacity, LAN topology, WAN circuits, floor plans, and wire closet layouts.

Workstation Installation

CIO/OFT delivers, sets up, and connects new workstations to the network. Smaller deployments are handled by existing staff; larger workstation deployments are outsourced in conjunction with the customer Agency. CIO/OFT monitors activities of delivery or equipment vendors to ensure schedules & protocols are followed and any problems are resolved. CIO/OFT provides day of install support to ensure that any deployment related technical problems are resolved.

Terminal Installation & Removal

This service provides the addition/movement/removal of WMS dumb terminals, line printers and processors, and network connectivity at the request of the Agency.

CIO/OFT will:

- Coordinate updates with the Data Center
- Determine needs and install networking equipment required for terminals
- Deliver, sets up, connect, and test terminals
- Remove & dispose of terminals no longer in use

All requests must be submitted in writing a minimum of 45 business days in advance for installation and thirty days for moves and removals. Service does not include repair or diagnosis of malfunctioning equipment. Service is limited to agencies that negotiated this service at the time of function transfer.

Service increases physical network security and limits the connection of unauthorized devices from accessing the network. Additional network security is provided by ensuring a connected workstation is current, in terms of operating security patches and anti-virus signatures, the anti-virus program is executed, and the workstation is not connected to another network.

ENDPOINT SECURITY

Service is available 24x7x365. The support for this service is available during Standard Business Hours unless otherwise negotiated. Please refer to the service description for 24x7x365 LAN/WAN Maintenance & Support for details on extending support for this service.

Service provides multiple functions related to maintaining the integrity of the customer network. While the focus is on client security, compliance with the State and CIO/OFT security policies and standards is extended to the entire network including the infrastructure. This service provides installation of appropriate security products, monitoring, and incident response.

CIO/OFT will provide a multi-layered group of services to ensure endpoint security. These services will include:

- Workstation and server Anti-virus software
- Anti-spyware detection and removal
- Client anti-spam control
- Patch management (assessment and remediation)
- Vulnerability assessment and protection
- User/computer account management

Workstation and Server Anti-Virus and Anti-Spyware

Both Client and Server Anti-virus and Anti-spyware Software is provided and installed and updates to signatures are distributed through a hierarchy of servers. These signatures are released by the vendor, at a minimum of once a week with interim updates being pushed out if necessary to combat a mounting threat. Specific actions include:

- Installing anti-virus/antispam software on workstations when needed
- Configuring workstations to proper local network servers for signatures and configuration updates
- Coordinating the remediation of workstation virus/malware infections with Level II team and customer
- Remediation of workstations/servers experiencing anti-virus product problems (service shutdown, lack of signature updates, etc.)
- Performing extensive proactive anti-virus console monitoring.
- Responding to vendor virus alerts taking actions needed including emergency distribution of new virus signature files
- Upgrading product levels
- Testing anti-virus product functionality on new workstation images
- Auditing sites to determine status of product on workstations within site and take corrective actions as appropriate
- Coordinating product installations on servers

User/Computer Account Management

Service allows the monitoring of computer and user accounts, including the disabling of accounts no longer needed, to prevent unauthorized access to the CNS network and systems.

With this service CIO/OFT will:

- Provide regular user/computer account analysis to determine usage
- Delete computer and user accounts, and mailboxes as needed

Patch Management and Assessment

Patch Management is provided for the operating system and commercial applications installed on an image.

CIO/OFT will:

- Provide a regularly scheduled assessment of patching requirements for all components of the basic image (Operating System and General Office products)
- Provide vulnerability analysis for Microsoft security patches
- Approve a patch deployment and auditing results
- Coordinate an Agency Remediation workgroup

Network Integrity/Security Incident Response

This service provides multiple functions related to maintaining the network integrity of the customer network. The focus is on maintaining client security compliance with State and CIO/OFT security policies.

CIO/OFT will:

- Review new services or changes to services related to network security
- Review and analyzes non-virus alerts as to the impact on Customer Networking Solutions and the Data Center (e.g. networking equipment vulnerabilities)
- Review and approves Firewall Rule requests
- Provide information related to Agency requests regarding investigations of misuse of State services provided by CNS
- Provide IDS incident investigation and response

Endpoint Vulnerability Assessment (Under Development)

Using monitoring and diagnostic tools, CIO/OFT will test and assess vulnerabilities to workstations, servers, and devices on the customer network and provide remediation to comply with policies set by CIO/OFT, CSCIC, and customer Agencies. CIO/OFT performs an in

depth proactive and reactive vulnerability analysis of targeted workstations or servers, and reports/patches discovered vulnerabilities as required.

TRANSACTION TERMINAL SECURITY SYSTEMS

Service is available 24x7x365. Support for this service is available during Standard Business Hours unless otherwise negotiated. Please refer to the service description for 24x7x365 LAN/WAN Maintenance & Support for details on extending support for this service.

Service provides application support for TTSS, a custom Unisys mainframe security package. This includes COBOL programming and maintenance of file structures for this application. This service provides support to County LAN administrators in utilizing the application.

SHAREPOINT

The CIO/OFT SharePoint service provides a turnkey, fully managed implementation of the Microsoft Office SharePoint 2007 web publishing and collaboration platform. CIO/OFT currently offers one level of SharePoint Service (SharePoint Standard), but anticipates offering additional service levels with additional features and capability in the future.

The SharePoint Standard Service consists of:

- Unique, agency specific URLs for SharePoint Sites
- A multi-tenant, shared farm infrastructure.
- Access to SharePoint sites via the NYeNet or Internet using authenticated access.
- All standard SharePoint application features
- Individual "My Site" capability with 100MB Quota
- Outbound Email capability (Inbound Email requires a NYSeMail Mailbox for each mail-enabled library)

ORDER PROCESS

CIO/OFT provides a formal service request intake process to ensure Agency requests are properly managed and fulfilled with a high level of satisfaction and a high quality of experience for the Agency.

The service request process includes the receipt, review, referral to the appropriate business unit, evaluation and determination of the requests prior to a response to the customer. This process typically takes 3 days.

CIO/OFT will:

- Follow a process to ensure requests are received, managed, tracked, assigned, and acted upon
- Provide designated Agency representatives access to an automated system for submitting service requests and receiving “request of receipt” notifications
- Assign requests to appropriate technical group for prompt action
- Provide designated Agency representatives the ability to track and query the status of their requests online
- Consistently update status requests to ensure proper tracking of requests
- Provide a timeframe of an estimated completion date of actions for request
- Maintain information regarding completed/closed requests

ROLES AND RESPONSIBILITIES

In order to achieve a successful service delivery relationship CIO/OFT and the Customer Agency have roles and responsibilities.

CIO/OFT will:

Network Operating Services: Administrative Model

- Evaluate the need for additional organizational (OU) structures within two business days
- Provision new organizational (OU) structures within two business days
- Apply security to organizational (OU) structures within one business day
- Delegate provisioning capabilities within two business days
- Plan and consolidate the moving or deleting of organization (OU) structures within fifteen business days

Network Operating Services: Provisioning

- Provide user manual for using the provisioning tool
- Provide standardized reports
- Provide ad-hoc reports as requested through Service Requests
- Investigate and triage problems with a provisioning tool within three business hours

Internet Access

- Evaluate and block inappropriate and malicious websites within one business day
- Evaluate and respond to requests for changes to proxy access within fifteen business days
- Evaluate requests and update changes to site filtering within five business days

Data Communications: Remote & Core Network – Network Performance Monitoring

- Monitor Bandwidth utilization and network errors for all circuits
 - If bandwidth exceeds threshold, a detailed analysis will be conducted within two business days. Circuit upgrade or other remediation will be initiated at the end of the analysis.
- Review circuits exceeding pre-defined thresholds
- Provide copies of reports or problem sites as requested

Data Communications: Remote Networks – Network Service Requests

- Conduct an initial evaluation of the Service Request within five business days
- Schedule a meeting to gather additional requirements within five business days
- Gather additional requirements within ten business days
- Complete research and drawings in a timeframe dependent on the scope of the work

Data Communications: Firewall and DNS Network Service Requests

- Complete service requests within ten business days after a fully completed SR is received

SSLVPN (for new or modified application access)

- Complete service requests within eight weeks, provided the customer Agency supplies the required information and allocates the necessary resources for testing

Workstation Configuration and Management Support

For SOFTWARE DISTRIBUTION

- Evaluate Operating System and office hot fixes or other updates within three business days
- Coordinate Agency testing of hot fixes with customer Agencies within ten business days
- Deploy OS hot fixes and updates to 90% of the workstation population within five business days

- Develop and test specialized software packages to meet customer requirements within forty business days, depending on package complexity

For WORKSTATION IMAGE CREATION & MANAGEMENT

- Evaluate service request within five business days
- Update OnelimageNYS to support new hardware (if applicable) within five business days
- Test updated OnelimageNYS with new hardware (if applicable) within two business days subject to hardware availability
- Customer and/or vendor testing of new image within four business days
- Delivery to installation vendor or customer within one business day

For INSTALLATIONS AND TECHNICAL SERVICES CIO/OFT will provide the following service levels:

- Respond to service request within three business days
- Fill in the Survey Request within thirty to ninety business days
- Remediate workstations and servers experiencing infections within one business day
- Scan all workstations for infections daily
- Scan all servers weekly

- Upgrade signature files weekly or as vendor releases

Global Services: File Share

- Evaluate service requests for disk resources within two business days
- Address service requests to configure or expand disk resources within five business days
- Investigate and triage, if a home directory server is unavailable, within three business hours

Customer Agency will:

- Maintain the integrity of the network with their business partners
- Participate in the Change Control Board
- Invite CIO/OFT staff to Agency strategic planning discussions or meetings
- Appoint an Agency representative and an alternate for consultation with CIO/OFT
Agency representatives and/or alternates shall be available 24x7x365 via telephone or pager to CIO/OFT
- Wire for LAN service, including PC/printer patch cables at the remote site

Site Contacts

Provide a list of site contacts to CIO/OFT Customer Relations. It is the Agency's responsibility to keep this list current.

Service Requests

Be responsible for following the appropriate procedure when making requests for service. These requests must be formatted as Service Requests (not trouble tickets through the CCC). Trouble tickets will not be honored as Service Requests.

Training

Provide education and training of its staff on the use of the desktop applications. The CIO/OFT Technology Academy can arrange additional training for a fee.

SUPPORT

Project Management

CIO/OFT provides project management support for CNS customers' projects to ensure Agencies' project goals are met. This offering provides the customer with a single point of contact to manage and coordinate all phases of a software, network or workstation deployment project. Projects typically involve multiple participants from a variety of organizations, including customer teams, CIO/OFT service providers, vendors, landlords, electrical & cabling contractors, and other support teams.

CIO/OFT will assign a dedicated Project Manager to the project.

The CIO/OFT follows the project management methodology as outlined in the NYS Project Management Guidebook and the CIO/OFT Project Process Checklist, which incorporates CIO/OFT's internal processes. CIO/OFT follows its Project Portfolio Management process, which evaluates and selects projects that meet the strategic goals of an Agency. In addition, CIO/OFT assists all CNS Program Areas in managing their projects to successful completion and does the same for some major operational activities.

CIO/OFT will:

- Ensure the project scope clearly defines deliverables and what will be produced
- Create a project schedule that defines project activities, durations, dependencies, required resources, and milestones
- Monitor the status of issues and projects and produces logs and reports to ensure stakeholders are informed and activities of project participants are coordinated. Reports will include major milestones and major issues.
- Work with the project stakeholders and participants to ensure all the necessary adjustments in the project's scope are documented and completed
- Inform stakeholders and helps seek resolution where possible if the project is falling behind schedule

Operation Support Levels II and III

CIO/OFT provides advanced technical support for a variety of technical issues to Agencies for the services identified in this document. When Level II support is unable to resolve an item, the item is escalated to Level III support.

CIO/OFT will:

- Provide resolution on trouble tickets escalated from Level I Customer Care Center through the ticketing system.
- Work with vendors to resolve problems with workstations, servers, and network equipment at remote sites
- Assign Level II help tickets to appropriate staff for review and action. Some steps taken may include, but are not limited to:
 - Analyzing and referring unresolved tickets to the appropriate group for triage
 - Returning incorrectly assigned tickets to the CCC for proper reassignment
 - Identifying a ticket as a problem or a request for new service
 - Assisting the CCC in identifying error message trends and reoccurrences
 - Returning tickets to the CCC upon resolution for closure in the ticketing system
 - Contacting affected Agencies to further define a problem and verify information provided to take necessary steps toward resolution
 - Addressing problems with Agency LAN Admin
 - Accessing system utilities
 - Providing internal reports to track requests for image CD's
 - Identifying the source of hardware problems to reduce problem occurrences
 - Providing training to LAN Administrators

Level III Service

CIO/OFT will:

- Provide problem resolution on data communication areas as well other network issues (e.g. slow symptoms) referred from Level II
- Review ports, settings, routing, and perform protocol analysis
- Review historical reports for trend setting, firewall rules, and access control
- Maintain and upgrade equipment including, but not limited to switches, routers, and firewalls.
- Troubleshoot potential problems with network wiring
- Review logs of network devices in an effort to identify problems and develop solutions.
- Perform network protocol analysis
- Establish a base for network performance for trending purposes, patterns, and bandwidth use
- Maintain device configuration (e.g. turn on a service)
- Maintain Network Time Protocol devices
- Identify underperforming equipment and plans design changes and replacements as needed

- Generate and reviews daily reports on network health
- Generate reports of circuit performance on bandwidth utilization, accessibility (circuits up), and circuit errors
- Provide rollout reviews based on number of users at site, provides Level III or install team to complete rollout review, assuring circuits are sized properly
- Work with vendors to solve problems on workstations, servers, and network equipment at remote sites
- Work with on-site vendors on site if chronic circuit problems occur

Local Sites Power Shutdown Assistance

In the event of a power shutdown, CIO/OFT will assist in completing the shutdown of data communications equipment, servers, and PCs. When power is restored, CIO/OFT will then provide assistance to ensure previously powered down devices are operating correctly.

Day of Install Support

CIO/OFT will:

- Provide support for vendor installs or Infrastructure installs at remote sites
- Ensure that Level I support properly triages and refers problems as warranted
- Generate an internal email ticket to the Coordination Center and contacts installers at the site to work to correct problems (e.g. change permissions, test and check status, security, profile etc.).
- Ensure that the appropriate project manager is properly advised

Customer Coordination for Project Rollouts

CIO/OFT provides a Customer Coordination service for Agencies that need to rollout projects for their customers. The Customer Coordination group works with CIO/OFT's Customer Relations Office, the CNS PMO Office, and the Agency's Project Manager to ensure proper communication and coordination occurs to support the successful launching of a new or upgraded product. This team responds and interacts directly with customers at the time of a project's rollout, managing the flow of communication.

CIO/OFT will:

- Assist in planning the communication required to support the project rollout
- Ensure that the communication is accurate and in understandable terms for the customer
- Distribute communications via letters, phone calls, or emails to the proper customers at the appropriate time to inform the customer of upcoming install events, and best coordinate with the project rollout

- Track and react to customer responses Appropriately
- React to incoming issues and problems communicated on the day of install, taking prescribed steps or referring problems to the appropriate resolver
- Recognize common patterns of difficulty, issues, and trends, resulting from communications with customers, and refers these to the Project Manager or other appropriate party
- Participate, as required, in closeout analysis of the project communication

COMMUNICATION

Network Operating Services: Provisioning

CIO/OFT will:

- Provide user manual for using the provisioning tool
- Provide standardized reports
- Provide ad-hoc reports as requested through Service Requests

Endpoint Security: Workstation and Server Anti-Virus and Anti-Spyware

CIO/OFT will:

- Provide weekly reports of protection status and infections

Global Services: Operation Support Level II and III

Customer Care Center tickets will be updated on a regular basis with relevant information. Service is available during normal business hours. CNS Level II will provide the following level of service in response to tickets that have been referred from CCC Level I.

- Investigation and triage will begin within 30 minutes for Severity 1 tickets
- Investigation and triage will begin within three business hours for Severity 2 tickets
- Investigation and triage will begin within three business days for Severity 3 tickets

Customer Care Center (CCC)

Prime time hours of operation are 7:30 A.M. to 5:00 P.M., Monday through Friday, State holidays excluded. Only during this time period will technical staff be available to conduct investigations, resolve outages, and work with users/vendors and others to maintain availability for all users in accordance with CCC Service Detail Information

<http://www.cio.ny.gov/assets/documents/SLA/CustomerCareCenterFeatures.pdf>. Severity Level 1 problems will be supported in a call back system during non-prime hours.

Once the CCC is aware of a Severity 1 or Severity 2 incident, the CCC Incident Management Team automatically notifies impacted customers and Resolver Groups as well as technical and management groups, as defined by customer preference, when an incident occurs.

Severity 1 incidents for any assignment group are monitored by L1 OFT CCC Incident Management. Severity 1 notifications include Initial notification, hourly updates, significant updates (as needed) and restored notifications and are sent by the Incident Management Team.

Severity 2 notifications include an Initial notification, 1 hour update, 4 hour update, 8 hour update, significant updates (as needed) and restored notifications.

The major difference between a Severity 1 and a Severity 2 is the frequency of incident status updates required.

There will be no pager or email notification, and NYS resolvers will perform proactive checks for Severity 3 incidents.

See additional information on the Customer Care Center at http://www.cio.ny.gov/customer_care_center

General

CIO/OFT will:

- Provide standardized reports including but not limited to:
 - a. All users in a particular location or Organizational Unit
 - b. All users with particular jobs
 - c. All users in a particular office
- Provide ad hoc reporting capabilities

LEGAL AND SECURITY ISSUES

Security

Agencies are responsible for:

- Providing Security Coordinators
- Informing staff and partners of security policies
- Working with CIO/OFT's ISO
- Advising CIO/OFT of any audits relevant to CIO/OFT services
- Complying with and enforcing CIO/OFT and OCSCIC security policies
- Informing CIO/OFT concerning violations of policy and procedures relevant to services
- Maintaining current user status
- Properly applying and using end-user and administrative rights
- Requesting and receiving approval from CIO/OFT before adding equipment to the network

HOW RATES ARE CALCULATED

NOS Authentication Metric:

This service is billed by:

- Flat rate per account
- Counts include the following (whether the account is active or disabled):
 - All user accounts
 - Resource Room accounts
 - Training accounts
- Excluded accounts are:
 - Administrator accounts
 - Service accounts

NOS Authentication Rate Detail:

On the third Wednesday of each month, Active Directory is queried for the total number of users in each organizational unit. Counts are aggregated by agency, based on the segment of the AD in which the user account resides.

Business rules that determine “account ownership” are applied as below:

1. Objects in OUs wholly attributable to agencies are assigned to that agency
2. Objects in AD HSEN\All Users\Agencies\HRA are assigned to OTDA
3. Objects in AD HSEN\All Users\ Counties\ACS, plus user accounts in AD HSEN\All Users\Agencies Voluntaries (excluding HRA) are assigned to OCFS
4. Objects in AD HSEN\All Users\Counties (excluding ACS and HRA) are assigned according to the following formula:
 - a) 40.5% of the user accounts are assigned to OCFS
 - b) 39.5% of the user accounts are assigned to OTDA
 - c) 20.0% of the user accounts are assigned to DOH

NOS Centralized File and Print Metric:

Flat rate per gigabyte of logical storage on core FNP servers, based on agency consumption.

NOS Centralized File and Print Rate Detail:

On the third Wednesday of each month, logical storage consumption on the core FNP servers is assessed. User data is assigned to agency based on the segment of the AD in which the user account resides. Other data is mapped to agency based on identified ownership. All data quantities are then summed by agency.

NOS Remote File and Print Metric:

Flat rate per remote FNP server deployed.

NOS Remote File and Print Rate Detail:

On the third Wednesday of each month, Active Directory is queried for the total number of FNP servers in each organizational unit. Counts are aggregated by agency, based on the segment of the AD in which the server resides.

The server count is multiplied by the applicable rate.

Note: There are a very small number of servers that are shared by multiple agencies. In each case, the agency that manages the server has the largest percentage of usage

Internet Access

There are four shared levels of proxy access:

1. Proxy Full – allows full access to the Internet except to those websites in which filtering software denies access to because of illegal, malicious, and inappropriate content.
2. Proxy Limited – allows access limited to an approved list of categories allowed through filtering software. This group provides greater access than the Proxy Restricted group, but is more limited than the Proxy Full access group.
3. Proxy Restricted – allows access to a restricted list of pre-approved work-related (mostly governmental) sites. This restricted access has historically been called the “GOER list”.
4. Proxy Block - allows access to only Intranet sites, but no access to the public Internet. This category is used in cases where a decision has been purposefully made to prohibit Internet access. (e.g. – clerical staff, vendors, history of misuse, disciplinary action, etc.). There is no cost for users with Blocked Internet access.

In addition to the shared groups, the content filtering software can be customized to enforce Internet usage policies based on the needs of each agency/organization.

The service includes a delegated reporting capability for agency Information Security Officers (ISOs) which can be used for investigations and to verify appropriate use.

In the monthly billing, this service appears as line item: **IA – Internet Access**

Metric:

Flat rate per user account.

Rate Detail:

On the third Wednesday of each month, Active Directory is queried for the total number of users in each organizational unit having Internet Access rights. Counts are aggregated by agency, based on the segment of the AD in which the user account resides.

Note: There is no charge for users restricted to the Intranet only - Proxy Block. “Account Ownership” is detailed on page 30.

Layer 2 Devices, Small/Medium/Large Layer 3 Devices and Circuits

In the monthly billing these services appear as the following line items, with R1 -R3 designating device categories:

- R1 – Layer 2 Devices per 24-ports
- R2 – Small/Medium Layer 3 & Small e-port Termination Devices
- R3 – Large Layer 3 Devices
- CT – Circuits

Metric:

Networking equipment is divided into three equipment categories, and charges are based on the actual count and category of equipment installed.

Circuits are billed at the NYeNet rate, plus overhead.

Rate Detail:

On the first workday following the billing month, an inventory database is queried to obtain the quantity, category, and location (site) of network equipment. Equipment for each site is grouped and counted according to the equipment categories listed above (R1 – R3). The count for each category is multiplied by the applicable rate and a site total is obtained by summing all categories. Site charges are assigned to agencies in the following manner:

1. Remote sites where there is only one agency present are charged in their entirety to that agency.
2. Remote sites that are shared will have charges allocated in direct proportion to the total number of PCs (workstations and laptops) and “green screen” terminals owned

by agencies at the site. PC counts are generated from Workstation Rate information. Terminal counts come from equipment inventory.

3. Shared infrastructure site charges are allocated to all agencies in direct proportion to their count of PCs and “green-screen” terminals relative to the total count in the environment.

Circuits will be billed as NYeNET charges plus overhead. Circuit charges are assigned to agencies in the following manner:

1. Circuits at remote sites where there is only one agency present are charged in their entirety to that agency.
2. Circuits at shared remote sites are charged in direct proportion to the total number of PCs (workstations and laptops) and “green screen” terminals owned by agencies at the site. PC counts are generated from Workstation Rate information. Terminal counts come from equipment inventory.
3. Circuits at shared infrastructure sites are charged to all agencies in direct proportion to their count of PCs and “green-screen” terminals relative to the total count in the environment.

24x7 LAN/WAN Maintenance and Support

Extends prime shift maintenance and support to 24X7X365 for equipment and Wide Area Network Services at a site. In the monthly billing, this service appears as line item:
SP – 24 x 7 Support

Metric:

Each site is assessed a monthly base charge for this service. An additional usage charge is assessed for off-hours service used.

Rate Detail:

The 24x7x365 LAN/WAN Maintenance and Support is charged to the agency or agencies requesting this service for a site. Charges are comprised of the following:

1. The monthly base charge consists of the base vendor “stand-by” rate determined by the maintenance contract, the CNS on-call staff cost, and the optional uplift maintenance cost for CNS managed servers. The vendor “stand-by” cost is regionally based and prorated among sites participating within a region. On-call CNS support is prorated on a statewide basis.
2. Usage charges are dependent upon the number of hours needed to resolve incidents.

Secure Individual Remote Access (SIRA)

Metric:

Flat rate billed at one unit per configured user. Users entitled for multiple agency access will result in a proportional charge to each agency ((user / # of different agency memberships) * rate).

Rate Detail:

Each agency controls user membership for their respective AD groups or NYSDS attributes. User membership is collected from each of the two directory stores once a month resulting in a single charge, for the authorizing agency, for each configured user. Users entitled for both SSLVPN and Client VPN access will incur a single charge for both services. Users entitled for multiple agency access will result in a proportional charge to each agency ((user / # of different agency memberships) * rate).

Workstation Configuration Management and Support

In the monthly billing this service appears as line item: **WS – Workstation**

Metric:

Flat rate per workstation

Rate Detail:

On the third Wednesday of each month, Active Directory is queried for the total number of computer objects in each organizational unit. Counts are aggregated by agency, based on the segment of the AD in which the computer object resides.

Business rules that determine “workstation ownership” are applied as below:

1. Workstations in OUs wholly attributable to agencies are assigned to that agency
2. Workstations in AD HSEN\All Users and Computers\Agencies\Human Resources Administration (HRA) are assigned to OTDA
3. Workstations in AD HSEN\All Users and Computers\ Counties\Administration for children services (ACS) are assigned to OCFS
4. Workstations in AD HSEN\All Users and Computers\Agencies (excluding HRA) are assigned to OCFS
5. Workstations in AD HSEN\All Users and Computers\Counties and AD HSEN\All Users and Computers\Lost Computers are matched to an agency using a CNS inventory table populated with the following data:
 - a) Workstation inventories provided by OCFS, OTDA, DOL and DOH.

- b) CNS Workstation rollouts for customer agencies, as documented in the Order Entry System.
- c) Inventories of agencies such as St. Regis Mohawk Tribe, which contain only OCFS PCs.

RESOURCES

Service Level Agreement Home Page

<http://www.cio.ny.gov/SLA.htm>

Customer Networking Solutions Rate Detail

<http://www.cio.ny.gov/assets/documents/SLA/RatesDetailNetworks.pdf>

Customer Care Center Features

<http://www.cio.ny.gov/assets/documents/SLA/CustomerCareCenterFeatures.pdf>

Customer Care Center Home Page

http://www.cio.ny.gov/customer_care_center

Customer Relations Managers listed by State Agency

<http://www.cio.ny.gov/support/ContStateCRMs.htm>

CONTACT US

Customer Relations Managers listed by State Agency

<http://www.cio.ny.gov/support/ContStateCRMs.htm>

Contact CIO/OFT Customer Relations Managers or the Customer Care Center at

1-866-789-4638 or 518-402-2537

When You Call

Option 1: Technical Support

Additional Choices:

1. Customer Care Center
2. Data Center Operations
3. NYeNet Network Operations Center (NOC)
4. Voice Services

Option 2: State and Local Government Customer Service (for Customer Relations Managers)

Option 3: New York State Directory Assistance Operator

OR by E-Mail at: customer.relations@cio.ny.gov