



**Correctional Service Canada
Facilities Branch
Electronics Security Systems**



July 27, 2015

**STATEMENT
OF
TECHNICAL REQUIREMENTS**

CCTV Network and Video Storage Upgrade

AT

**Atlantic Institution
Dorchester Medium and Minimum Institution
Springhill Institution
Nova Institution**

AUTHORITY

This Statement of Technical Requirements is approved by the Correctional Service of Canada for the upgrade of the CCTV Network and Video Storage at Atlantic, Dorchester, Springhill and Nova Institutions. Recommended corrections, additions or deletions should be addressed to the Design Authority at the following address:

Director, Electronic Security Systems
Correctional Service of Canada
340 Laurier Avenue West,
Ottawa, Ontario
K1A 0P9

Prepared by:


Larry Carter
Chief Electronic Security Maintenance
Electronic Security Systems

Approved by:


Marc St-Amand
Director,
Electronic Security Systems

TABLE OF CONTENTS

ABBREVIATIONS.....	4
1.0 INTRODUCTION.....	5
1.1 General.....	5
1.2 Scope.....	5
1.3 Requirement.....	5
1.4 Site Visits.....	6
1.5 Technical Acceptability.....	6
2.0 APPLICABLE DOCUMENTS	7
2.1 Applicability.....	7
2.2 Applicable Standards and Specifications	7
3.0 OPERATIONAL CRITERIA	8
3.1 General.....	8
3.2 System Specifics.....	8
4.0 TECHNICAL REQUIREMENTS	9
4.1 Concept of Operation	9
4.2 Existing Camera System Verification	9
4.3 Existing Camera System Configuration	9
4.4 System Installation	9
4.5 Removal Equipment and Cables.....	11
4.6 Cameras.....	11
4.7 Expandability.....	11
4.8 Network Infrastructure	12
4.9 Equipment Racks.....	15
4.10 Network Video Recorder	15
4.11 Uninterruptible Power Supply	18
4.12 Network Video User Station.....	18
4.13 Fibre Equipment.....	18
5.0 ADDITIONAL REQUIREMENTS	18
5.1 Operator Training.....	18
5.2 Maintenance Training.....	18
5.3 Manuals.....	19
5.4 As-Built Drawings.....	19
5.5 Testing.....	19
5.6 Institution Operations	20
5.7 Institution Address.....	21
5.8 Integration Responsibility	21
5.9 Security.....	21
5.10 Schedule.....	21
5.11 Safety.....	21

Appendix A - Maintenance Handover Report Form

Appendix B - Safety Regulations for Security Electronics Contractors Working at CSC Institutions

Appendix C- CPIC Form

Appendix D- List of existing Cameras

Appendix E- List of existing User Stations and monitors

Appendix F- CCTV network Drawings

ABBREVIATIONS

The following abbreviations are used in this specification:

ATP	Acceptance Test Plan
CCTV	Closed Circuit Television
CER	Common Equipment Room
CMO	Correctional Manager Operations
CPU	Central Processing Unit
CSC	Correctional Service Canada
DA	Design Authority
FOV	Field Of View
IP	Internet Protocol
P/T/Z	Pan/Tilt/Zoom
MCCP	Main Communications and Control Post
NVR	Network Video Recorder
NVUS	Network Video User Station
PIDS	Perimeter Intrusion Detection System
PIU	PIDS Integration Unit
POE	Power Over Ethernet
REPO	Regional Electronics Program Officer
STR	Statement of Technical Requirements
TER	Terminal Equipment Room
UPS	Uninterruptible Power Supply

1.0 INTRODUCTION

1.1 General

Correctional Service Canada (CSC) has a requirement to upgrade the existing Closed Circuit Television (CCTV) Network at Atlantic, Dorchester, Springhill and Nova. This upgrade will include the following; CCTV cameras, network video user stations, network video recorders and the replacement of existing 62.5 micron fibre infrastructure. The fibre infrastructure will be replaced with OM 3 50 micron fibre, this fibre network will be terminated in the electronic security equipment cabinets located in the TERs and CERs within the institutions. The CCTV network switches will also be upgraded. The existing network video recorders shall be replaced with a Storage Array Network (SAN) system. The new equipment is to be compatible with and integrated into a Genetec, Security Centre System. The existing Genetec Omnicast software will be upgraded to Genetec Security Center.

The primary purpose of the CCTV system is to provide video surveillance and recording. The CCTV system is monitored and managed from the living unit control posts and the MCCP.

Atlantic Institution is a maximum security institution located at Renous, NB. Dorchester Penitentiary is a medium and minimum security institution located at Dorchester, NB. Nova Institution is an institution with multi-levels of security located at Truro, Nova Scotia. Springhill Institution is a medium security institution located at Springhill, NS.

1.2 Scope

The contractor must supply, install, test, and provide operational and maintenance training on the new installed cameras, CCTV fibre network infrastructure, network switches, user stations, video storage equipment and the upgraded Genetec Security center software, as described in this STR. The contractor must provide acceptable documentation for the operation and the maintenance of this system. The replacement of existing CCTV equipment must be 100% integrated into Genetec Security centre.

1.3 Requirements

This STR will also indicate the extent to which both general and particular CSC specifications are applicable to the implementation of this requirement. Bidders must comply with the STR and the listed specifications and standards unless identified in this STR. The STR takes precedence over the subordinate documents such as a Statement of Work, a Specification or a Standard.

1.4 **Site Visits**

The Design Authority, or their authorized representative, will coordinate a mandatory site visit, and identify to the potential bidders the exact locations of the user interfaces, the system servers, archivers or control interfaces, power supplies, interconnecting cable and any other associated electronic equipment. Wherever possible, drawings and documentation will be made available.

The visits may be useful to determine:

- a. The space, power, spare cable pairs, etc. which are available at equipment mounting locations at these sites,
- b. The conduit and cable requirements for power, video and control signals to the cameras and other equipment locations at these sites,
- c. Condition of existing power, video and control cables,
- d. General layout and operating environment at the site.

1.5 **Technical Acceptability**

The CSC operational environment is unique for its diversity of locations, climate exposures and the physical restrictive construction techniques of penal institutions. Maintaining national security, the safety of staff and offenders alike is CSC's commitment to the government and public. Electronic security systems operating in this unique environment must maintain very high standards of dependability and reliability.

The CSC Engineering Services Division has established Statements of Work (SOW), technical specifications and standards for security electronic systems, which are based on very specific, and restrictive operational performance criteria. Technical acceptability of these systems means that the systems equipment and components comply with the pertinent CSC SOWs, specifications and standards.

2.0 APPLICABLE DOCUMENTS

2.1 Applicability

The provisions contained in the documents listed in the following paragraphs will apply to all aspects of this requirement, unless these provisions have been exempted or modified by this STR.

2.2 Applicable Standards and Specifications

- a. ES/SOW-0101 Electronics Engineering Statement of Work, Procurement and Installation of Electronic Security Systems
- b. ES/SOW-0102 Electronics Engineering Statement of Work, Quality Control for Procurement and Installation of Electronic Security Systems
- c. ES/SOW-0110 Electronics Engineering Statement of Work, Structured Cable Systems For Electronic Security Systems
- d. ES/SPEC-0006 Electronics Engineering Specification, Conduit, Space and Power Requirements for Security Systems for use in Federal Correctional Institutions
- e. ES/STD-0221 Electronic Engineering Standard, Fixed Network Colour Closed Circuit Television Camera
- f. ES/STD-0207 High Security Enclosure, Closed Circuit Television
- g. ES/STD-0227 Electronics Engineering Standard, LCD Colour Computer Monitor, Closed Circuit Television
- h. ES/STD-0228 Electronics Engineering Standard, Network Video User Station, Closed Circuit Television
- i. ES/STD-0229 Electronics Engineering Standard, Network Video Recorder, Closed Circuit Television
- j. ES/STD-0234 Electronics Engineering Standard, Indoor Network Colour Dome, Closed Circuit Television Camera
- k. ES/STD-0232 Electronics Engineering Standard, Outdoor Network Colour Dome, Closed Circuit Television Camera
- l. ES/STD-0235 Electronics Engineering Standard, Indoor Network Colour Panoramic, Closed Circuit Television Camera

3.0 OPERATIONAL CRITERIA

3.1 General

The contractor must supply and install new CCTV equipment to upgrade an existing digital CCTV system. The upgrade shall include the installation of new OM3 50 micron fibre and CAT5 or CAT6 termination bays, replacement of all CCTV Ethernet network switches, Network Video Recorders and Network Video User stations computers, Monitor and Cameras, to provide a complete CCTV network throughout the four (4) institutions. A number of existing cameras shall be reconfigured to support H.264. Provide and install new CCTV equipment cabinets as required that meet the requirements detailed in section 4.14 of this STR. The new CCTV archive array as detailed in this STR must be installed in a new or existing electronics equipment cabinet and configured to operate with the Genetec Security Center platform. The operational parameters of the installed equipment must meet the performance and operational requirements in accordance with the Specifications and Standards listed in paragraph 2.2.

3.2 System Specifics

This project will see a turn-key digital CCTV system installed at Atlantic Dorchester and Springhill institution. This system will be complete with all necessary mounts, cable dressing brackets and straps. All conduit and cable provided will meet CSC – Electronics standards and specifications. All new equipment provided must seamlessly integrate into existing digital CCTV equipment

3.2.1 Video Management System

The project shall result in a major upgrade of the existing GENETEC Omnicast 4.8 Video Management System to Genetec Security Center platform. The system upgrade requires that all network and camera hardware be properly programmed to be 100% compatible on a Genetec VMS platform. All Work on the VMS software, video storage solution, network support equipment must be integrated by a certified Genetec reseller employing trained and certified Genetec installation/integration technicians. Installation technicians Genetec certifications qualifications must be confirmed with Genetec.

3.2.3 Existing Equipment

Installation of this upgrade must not interfere with the operation of existing equipment and video recording at the Institutions without the explicit written permission of the contract authority.

3.2.4 Licences

All additional Genetec Omnicast licenses required for equipment provided as a result of this upgrade shall be provided by the contractor. This includes all camera, recording and fail over licences.

4.0 TECHNICAL REQUIREMENTS

4.1 Concept of Operation

4.1.1 Video Surveillance

Video surveillance of certain sensitive areas is required to maintain a safe and secure environment for both staff and inmates.

4.1.2 User Interfaces

All control functions such as selection and control of the Pan/Tilt/Zoom (PTZ) and spot monitor selection of a camera will be through the use of a mouse or touch screen. Playback, recording, searching or archiving of video to external media will be accomplished through the use of a mouse and keyboard.

4.2 Existing Camera System Verification

The institution has a camera system comprised of digital cameras which tie into computers using Genetec Omnicast software. Cameras are monitored and controlled at all Control Posts, Security Intelligence Office, MCCP and Crisis Centre.

The contractor must test the operational characteristics of all existing equipment and systems, whose equipment is in proximity to where work will be carried out or which will be reused, prior to removal or installation of any equipment and provide a written record of those tests for the Design Authority.

The contractor must identify any operational deficiency of equipment or else risk being held accountable for system deficiencies during the commissioning period.

4.3 Existing Camera System Configuration

Refer to appendix D and E for a list of existing CCTV network equipment currently installed at the four institutions. Given that the CCTV networks are constantly expanding; Updated block diagrams will be issued during the bidder's meeting indicating equipment locations, equipment models and quantities.

4.4 System Installation

The contractor shall supply, install and test a complete and fully functional IP based CCTV system. The CCTV system must meet or exceed all of the performance and operational requirements contained in the SOW's, specifications and standards listed in Section 2.2. Where there is a conflict between a published specification and this STR; this STR will be the document of reference. The existing CCTV system must remain operational throughout the installation of the new equipment. All integration must be coordinated with the institution's operational management in accordance to an Integration Plan which requires prior approval by the Technical Authority.

The contractor must provide a phased approach schedule. CSC requests that the network head end and all network switches are installed and tested before any work is scheduled for the ranges. It is requested that electrical work in the ranges be combined with the installation of new and replacement of existing cameras. All work must be completed on a range by range basis.

The contractor must avoid, as much as possible, the use of conduit in inmate accessible areas. The contractor must utilize existing pipe chases, existing conduit in the walls, etc., where possible. New lengths of conduit must be of the minimum necessary length. The contractor must install rigid conduit in all inmate areas. All newly installed conduits carrying video for this project must be identified, except in inmate accessible areas, by prominent labels with **BRIGHT GREEN** wording. These labels must be located at each end of the conduit run, on both sides of any penetration of a wall, and at 3.5 meter points along its length. Patching and painting must be done around new conduit installations, however painting the conduit is not required.

The deployment of this new CCTV switching infrastructure shall utilize the new OM-3 50 micron fibre installed as required under this STR

All data cables and data jumper cables (minimum 23 gauge), jacks and connector boots installed as part of this project, whether CAT 6 or fibre optic, must be BRIGHT GREEN in colour. All cables must be FT4 rated. All patch cables must be labeled at each end with **mechanically produced labels** designed specifically for cable labeling. All fibre optic strands must be terminated with connectors. All CAT6 premises wiring solutions must come with a minimum 10 year warranty on the connectivity between terminations on all premises cabling solutions deployed.

All patch cables are to be stranded cable with RJ45 connectors. All installed runs of CAT6 cable are to be solid conductor cable and terminated into patch panels in equipment racks. Cameras must be connected directly to installed cable either terminated with a TIA compliant CAT6 RJ45 solid conductor connector or a TIA compliant factory assembled stranded CAT6 pigtail with RJ45 connector on the end of the installed cable. Faceplates and patch cables for camera connections will not be acceptable.

An installed cable is any cable that is run through a conduit, run from one area in a building to another area or any cable that travels farther than the adjacent equipment cabinet in a series of cabinets. Note: Equipment cabinets must be abutting and without side panels to be considered adjacent. Conduit and/or cable trays are available between the cameras and TERs and CER.

Rigid conduit must be used in all inmate accessible areas e.g. walkways, low ceilings, and gymnasiums.

Media converters for long run outdoor connections may be either temperature hardened or installed in heated enclosures.

4.5 Removal of Equipment and Cables

4.5.1 Disposition

The contractor must remove all of the redundant cables, conduit and equipment located in and on various buildings. Note the existing 62.5 fibres, will not be removed and shall remain part of the institutional fiber backbone, care must be taken to ensure that any cables and conduits of other systems are not damaged. All electronic equipment must be handed over to CSC in good condition. The contractor must dispose of all of the removed cables and conduit off site in an environmentally friendly way.

4.5.1 Inventory List

The contractor must provide, to the DA, a list of all equipment to be removed 2 weeks prior to any equipment removal. This list will contain the following information as a minimum; location, make, model and serial number. The contractor must return all removed equipment to the local ADGA electronic maintenance workshop, where it will be inventoried and tagged for disposal. This information will be used to ensure the removal of the equipment from the maintenance contract, and its proper disposal.

4.6 Cameras

All new CCTV cameras will be powered via PoE over the interconnecting Ethernet cable, outdoor PTZ cameras may be powered by separate rack mount PoE, PoE+ or PoE++ injecting power supplies located at the closest NODE or electronics equipment cabinet to the camera. It is preferred all cameras are powered via PoE directly from the supporting network switch. Where separate PoE, PoE+ and PoE++ injectors are necessary they will be securely rack mounted, if more than 4 PoE injectors are necessary in a cabinet, they will be mounted into a manufacturer designed chassis designed specifically to host the injectors and reduce cabinet density.

All existing cameras that support operation in H.264 format shall be switched to operate in that format. Refer to Appendix E for detail of cameras that are to be upgrade and cameras that are to be reconfigured to H.264 format. The Field of Views for the replacement cameras will be as per the original FOV as approved in the Atlantic field of view manual. A copy of the Atlantic field of view manual is available on site for use during setup of the FOVs. The lenses must be of the same manufacturer as the cameras, or approved by the camera manufacturer. Unproven third party lenses are not acceptable.

4.7 Expandability

It must be possible to expand the system beyond the originally installed capacity through the installation of additional hardware. The system expandability must not be limited in this regard. It must be possible to use the digital backbone for other applications in the future, such as Voice Paging, Voice Intercom, Access Control, Door Control, etc. These systems may be installed by a different manufacturer than installed the original IP video system. A minimum of 50% spare capacity is required for expandability on the new distribution.

4.8 Network Architecture

The contractor must supply new and replace all existing network switches. Network switches shall be replaced on a location to location basis with the following exceptions, Dorchester, shall combine the network switches in building 7 rooms 110 and 310 to the TER in building 7 room 002. Springhill Institution shall combine the network switches in building 7 electrical room 159 to building 1 main CER room 112. Nova institution shall combine the network switches in the Electrical room 006 to the Main CER room 003.

CSC requires an upgraded network infrastructure capable of providing integrated support for multiple Electronic Security System (ESS) sub systems. Initially, for this deployment, this network infrastructure must support the deployment of CCTV cameras and associated client computers. The system must be expandable to scale to support additions to this CCTV network infrastructure and/or addition of further ESS sub-systems within the institution as required in the future. This network infrastructure must provide an integrated, end-to-end “virtualized” architecture for the systems connected to it, using state of the art techniques for the network operation and configuration as described in sections below.

The new network switching infrastructure must be sourced by one switch vendor with the ability to interface in a multi-vendor manner to other vendors equipment should future requirements deem this necessary.

CSC, ESS systems network traffic is predominantly streaming video from CCTV camera operation. The provided network infrastructure must be optimized for (H.264) multicast video operation for both cameras covered by this deployment and the addition of further cameras which may be added in the future; optimization including the perspectives of:

- simplicity and efficiency of protocols involved;
- efficient video streaming with required low latency, high bandwidth and network resiliency for predictable, always on connectivity;
- connectivity to the associated video management system (VMS), storage and viewing stations (NVUS).

The system must be capable of supporting thousands of independent streams. The system must be configured with readiness for sub-second failover recovery in the event of any failure, with no visible loss of data, once active-active links are deployed within the institution. The faster recovery is to maintain connectivity and avoid data or packet loss and minimize pixilation of video data.

The network infrastructure must provide an open system, multi-vendor capable, communication environment utilizing IEEE 802.1aq Shortest Path Bridging (SPB) to forward and control traffic between switches.

The new network switches to be provided must replace existing switches deployed for the support CCTV cameras.

The contractor is responsible to ensure the new switching infrastructure is fully integrated into the FAAS and PIU alarm and display systems.

The network is to be built primarily from stackable 48-port switch devices, with the use of 24-port and 8-port switches for lower capacity buildings

The contractor is responsible for taking all steps to minimize the number of network equipment devices required to minimize sparing requirements.

All switches must include QoS (Quality of Service) and security management capabilities. Each switch must have the ability to classify, mark and prioritize traffic into a minimum of 2 strict priority queues, and 6 weighted round robin queues on every port, and maintain QoS across the virtual / stack backplane. Classification controls and ACL (Access Control List) strategies must include the ability to sort traffic based on: MAC Address, 802.1Q VLAN ID, IP Address, TCP/UDP Ports, CoS (Class of Service), ToS (Type of Service), and DSCP (Differentiated Services Code Point).

The network infrastructure must provide a layer 2 SPB VID (VLAN identification) environment in which each ESS subsystem has its own allocated VID to provide for secure traffic segregation for each sub system and thus ease of monitoring, troubleshooting and maintenance. Each VID must be logically separate from any other and thus allow multiple services and systems to operate independently on the same wired infrastructure.

The network infrastructure must be capable of supporting flexible topology configurations e.g. star, full or partial mesh or ring topology to allow for optimal use of additional data paths as these become available and thus provide extra resiliency and readiness for redundancy in network connectivity connections.

The electrical contractor is responsible to confirm that all network switches within the network infrastructure are mountable in 19" mounting rail racks, and that the switches do not exceed the depth of communication racks and cabinets.

Core network

The core network must consist of a single core L2/L3 switch deployed in the CER and providing management of the SPB network. This core switch must be compatible with upgrade to a switch cluster, with a minimum of two switches acting as one logical switch, providing active-active switch operation and linkage capability once further fibre links are available at this institution. This switch cluster must provide high availability connectivity and links to the edge switching equipment.

This switch cluster must be a 19" rack mountable 1RU switch providing the capability to be configured with Layer 2 and layer 3 switching features.

The core switch and network infrastructure must support ease of provisioning via edge only device and service provisioning, providing ease of configuration at the edge devices automatically informing the network infrastructure of a move, add or change and not require core configuration when changes to the network are required. The edge only provisioning must be capable of adding a new device to the associated VID.

For network access control and security, the network system must provide software for automatic edge device authentication to ensure edge devices are compatible devices for installation, manage device permissions and monitor the health of connected devices.

The core-switch must support a minimum of 1 Gbps wire speed.

The switch must support end-to-end (system-wide) network infrastructure support for a flexible and robust, optimally high availability and reliable (Best in class mean time between failure) network (that is always on), with high throughput (1Gbp) and providing a lossless environment with lowest latency (<4ms) for an evolving, high performance CSC institution data center environment

The switch must provide hot-swappable power supplies with redundant fans.

Edge network

The edge switches must be stackable 48 (or where appropriate 24) port network switches utilizing 802.1aq SPB allowing for ease of future expansion of the network infrastructure and the capability for multiple connections into different switches in the stack utilizing load balanced network paths to provide an extra level of resiliency within the network in case of any switch failure. For more remote site locations with low port capacity connection requirements a compatible SPB 8-port switch must be used.

The edge switches must provide:

- L2/L3 switching
- 10/100/1000 Mbps switching
- 1GBps SFP+ uplinks (with migration option for 10Gb future uplinks) resilient, always on connectivity
- Wire-speed performance and non-blocking throughput to support a variety of applications including requirements for low latency, high bandwidth, reliable video surveillance
- Field replaceable redundant power supplies for increased resilience
- maximum POE wattage to support CCTV surveillance cameras deployed with capacity for further additions; must be able to concurrently deliver up to POE+ per port
- Flexibly support for IEEE 802.3af POE and IEEE 802.3at POE+ devices per port, optimized for video surveillance (including PTZ devices, HD)
- Provide one-touch edge provisioning for edge devices with any move, add or change communicated automatically throughout the network infrastructure
- capability (via stackable functionality) to add further network capacity as required without impacting current operational switching
- support for independent switch handling extended Ethernet reach to cameras in the mid-perimeter (two cameras extended to each tower)
- Support IEEE 802.1aq SPB
- Advanced QOS and prioritization
- Network access control (NAC) via device authentication software and IEEE 802.1x Port-based NAC
- Support for both IPv4 and IPv6 management addresses

The Edge switches must provide for edge-provisioning, automatically informing the rest of the network of the change/ addition, eliminating the need for manual configuration of the core switches when changes are made.

Network switches must be capable of device authentication, and include a management GUI interface for maintenance equipment.

Technical requirements:

- 350 W, 120 V power supply; POE switches are required to be able to concurrently deliver up to POE+ per port
- support up to 50 Ethernet ports (48 port version)
- software support for IPv4 and IPv6

Temperature range of operation: 0°C to 40°C

Operating humidity range: 0 to 95% relative humidity

The contractor is to supply network switches to meet the needs of all ESS network requirements.

4.9 **Equipment Racks**

The contractor must supply new equipment cabinets required to accommodate all additional equipment installed under this STR. Existing equipment rack space made available as a result of the upgrade can be used. The contractor is responsible for all costs associated to include sufficient cooling for all CCTV hardware. The contractor must provide a solution which includes venting through the exterior wall of the room.

4.10 **Network Video Recorder**

Required Server and SAN Storage Functionality

Supply a minimum of 169 hours of recorded video for all new and existing cameras.

The hardware platform must have the ability to run video management applications concurrently with shared storage on a common hardware platform using the VMware vSphere Hypervisor whereby;

Separate physical VMS servers are not required.

Separate physical failover VMS servers are not required.

Power and cooling for both server and storage functionality is contained within a common platform.

Applications running on each integrated platform must have access to the combined capacity of the storage in all platforms that are clustered together.

Applications running on each integrated platform must have access to the combined bandwidth of the storage in all platforms that are clustered together.

The integrated Server/SAN platform must support automated application recovery to reduce downtime.

Both storage and server operations must be resilient to an appliance failure.

Failover of the server application must be automatic in the case of an appliance failure

The integrated Server/SAN platform must support Windows Server and Linux operating system environments.

The platform must support Microsoft Storage Server for optional NAS share access.

The platform must support Linux running SAMBA for optional NAS share access.

Basic Storage configuration

Storage must be addressable by up to 128 external servers or hosts.

Storage must be IP attached via Gigabit Ethernet using commonly available networking configurations and equipment.

Storage must conform throughout to the iSCSI standard.

Storage must be SATA-based for cost effectiveness.

System must support SLC solid-state cache for database performance.

Storage system must be UL and CE certified.

Storage system must conform to and be deployable in industry standard 19" rack configurations.

Storage system must support at least 12TB raw storage per 2U (3.5") of vertical rack space.

Availability

Storage system must support high availability with no single point of failure causing loss of data or interrupting access to data.

Storage must protect data for up to five simultaneous disk failures with no loss of data or loss of access to data.

Storage must protect against loss of a storage appliance or controller with no loss of data or loss of access to data.

Storage must protect against loss of a networking path between servers and storage, including network interface card, cables and switches, with the ability Storage must support dynamic replacement of hardware components without interrupting access to data.

Storage must support the ability to replace disk drives without the need to interrupt data access.

Storage must support the ability to replace power supplies without the need to interrupt data access.

Storage must support the ability to replace fan modules without the need to interrupt data access.

Storage must support the ability to replace entire appliances without the need to interrupt data access.

Storage must support the ability to replace network switches without the need to interrupt data access.

Storage must support dynamic management features to ensure continuous data access.

Storage must be expandable by the addition of disk capacity without the need to interrupt data access.

Storage must be expandable by the addition of network bandwidth without the need to interrupt data access.

Storage must provide flexible, selectable data protection options.

Storage must provide enhanced RAID 6 data protection for critical data protection environments.

Data protection options must be selectable and configurable on a volume-by- volume basis.

Storage system must provide advanced data recovery methods to maximize data availability.

Storage systems must include dynamic sparing capability to allow immediate rebuilding of failed drives
System must conduct background disk data verification to ensure maximum data availability
System must have the ability to prioritize data recovery versus data access and to have that priority dynamically alterable before or during data recovery
System must have the ability to prioritize recovery tasks by volume
System must provide predictive sparing to identify poor performing drives in advance of failure

Scalability and Performance

Storage system must be scalable in capacity, supporting a single volume growth to 288TB; Capacity must be added to the system in modular increments of 12 or 24TB.
Capacity scaling must be non-disruptive allowing new capacity to be dynamically added to the system without interrupting access to data.
Physical capacity added to the system must be configurable into new volumes or added to existing defined volumes without the need to interrupt data access
Storage I/O must be scalable
Support up to 12 controllers; complete Active/Active.
System must support a minimum throughput of 2 Gigabits per second and 30,000 IOs per second.
System must allow additional bandwidth and I/O processing to be configured scaling to at least 24 Gigabits per second throughput and 360,000 IOs per second.
System must allow scaling of solid-state write cache to 600GB
Addition of I/O performance capability must be non-disruptive and not require data access to be interrupted
Storage system must support multiple storage hosts without the requirement for additional host software license charges
Storage system must support future capacity expansion with newer technology
System must provide a solid-state write-cache that scales across appliances. The system write-cache must protect in-flight data against loss of a complete appliance

Management

System must provide an easy-to-use graphical management capability
System must self-discover its hardware configuration
System must provide capacity and performance usage statistics
System must allow dynamic configuration of volumes
System must allow volume attributes including RAID type and volume size to be dynamically alterable without interruption of data access
System must have the ability to prioritize data migration versus data access and to have that priority dynamically alterable before and during data migration
System must provide administrator security controls
System must include a scriptable Command Line Interface
System must include advanced maintenance and manageability features.
System must log configuration changes and system events.
System must detect drive failures and graphically (via GUI) and physically (via lights) identify the

failing drive.

System must provide an audible alarm option.

System must detect controller failures and graphically identify the failing controller.

Simple Network Management Protocol (SNMP) traps have been increased thus providing more remote notification alarms to the PIDS and FAAS Display Units in the MCCP.

4.11 **Uninterruptible Power Supply**

The NVUS monitors are not required to be connected to a UPS, but must be connected to the institution's emergency power supply.

4.12 **Network Video User Station**

All NVUS must be rack mounted and installed in existing TER and CER rooms. Monitors, keyboards, mice, and joysticks must be remotely controlled to the user area. A NVUS must support a minimum of 9 video Streams and at least 2 monitor. . KVM extenders must be IP based. Where NVUS must be placed in an office or user area the NVUS noise levels must not exceed 50db at 3ft from the computer. NVUS video viewing streams must be identical to the, frame rate and bandwidth as the recording streams. Existing NVUS stations must be replaced with new. Each command post location must require the ability to control video monitor screens available for display viewing. The SIO must have the ability to retrieve and retain evidentiary data.

4.13 **Fibre Requirement**

Fibre installations must comply with ES/SOW-0110. All new fibres must be tested in both directions with an OTDR with all signal strength values documented and provided at Acceptance Testing. The contractor must replace and/or repair any video, power, conduit and junction boxes used to complete this project in accordance to the electrical code.

5.0 **ADDITIONAL REQUIREMENTS**

5.1 **Operator Training**

The contractor must prepare and present a one-day training course, in English, to two groups with five Operator/Trainers in each group, responsible for the operation of the equipment in accordance with the specification ES/SOW-0101 Statement of Work. The course must concentrate on the features and proper operation of the installed system. The course must be presented on the site within two weeks of the successful acceptance testing of the system.

5.2 **Maintenance Training**

The contractor must prepare and present a two-day training course, in English, to five persons responsible for the maintenance of the equipment. The course must concentrate heavily on the material contained in the technical manual and site manual. The course must be presented on the site within two weeks of the successful acceptance testing of the system.

The contractor is responsible to ensure that CSC maintenance technicians receive training to be able to provide 1st level monitoring equipment.

In the event of any failure of equipment under this STR, including the network switching infrastructure, the contractor is responsible for immediate resolution for resumption of full system operation. This must include provision of a three year warranty including a response time to a service call of within 4 hours.

In order to facilitate this, the contractor must be required to ensure appropriate maintenance support agreements are in place with the switch vendor to provide immediate support in the event of equipment failure. The contractor must provide proof of the availability of certified maintenance support.

5.3 Manuals

The contractor must provide the operator and technical manuals, in English, in accordance with the specification ES/SOW-0101 Statement of Work. The contractor must provide ten copies of the operator manual in English, and two copies of the maintenance manual in English to the site. The contractor must provide one copy of the operator manual in English and one copy of the maintenance manual in English to both the DA and the RTEO. Maintenance manuals must all include completed ATP forms. The contractor must provide copies of the completed Maintenance Handover Report Form contained in Annex A along with PDF versions included on a disk.

5.4 As-Built Drawings

The contractor must provide as-built drawings of the site installation in AutoCAD 2010 format and in accordance with specification ES/SOW Statement of Work. The contractor must provide two copies of the as-built drawings to the site, one to the DA and one to the RTEO.

5.5 Testing

- 5.5.1 The contractor must provide a detailed ATP to the DA, or his designated representative, by fax or email, for approval at least two weeks prior to the *start* of installation of the CCTV equipment and system.
- 5.5.2 The contractor must complete *one hundred percent* of the tests outlined in the ATP prior to the ATP testing being carried out by the DA.
- 5.5.3 The contractor must provide a *fully completed and signed copy* of the ATP to the DA, or his designated representative, by fax or email, at least two working days prior to the start of the final ATP testing. This copy of the ATP must include all of the results of the tests carried out in Section 5.6.2.

-
- 5.5.4 In the case where subcontractors have been used, the contractor must provide written confirmation that the work of their subcontractor has been inspected and verified. This verification must be sent to the DA or his designated representative, by fax or email, at least two days prior to the start of the ATP.
 - 5.5.5 Testing may be carried out by the DA, a designated representative or a third party contractor.
 - 5.5.6 The DA may repeat all of the ATP tests done by the contractor or a percentage of them. During the ATP, if an unacceptable level of failed tests are encountered, the ATP testing must be halted until the contractor has corrected the failures.
 - 5.5.7 If the DA during the ATP testing finds a minor deficiency that does not affect the operational effectiveness of the CCTV equipment or system, the ATP testing may continue. If a major deficiency is found during the ATP testing that does affect the operational effectiveness of the CCTV equipment or system; the testing must cease until the deficiency has been corrected.
 - 5.5.8 ATP testing must be done during normal working hours, 08:00 to 16:00, Monday to Friday. ATP testing at other times will only be done in an emergency situation.
 - 5.5.9 The DA or designated representative will sign-off on the ATP, upon the successful conclusion of the testing. Any minor deficiencies noted during the testing must be indicated on the ATP form. This signature indicates the Conditional Acceptance of the system.
 - 5.5.10 System must be subjected to operational testing for a period of two (2) weeks following the Conditional Acceptance of the system. CSC will formally accept the system from the Contractor at the end of this two (2) week period, but only if ALL deficiencies have been corrected.
 - 5.5.11 Any deficiencies noted by CSC during this two (2) week operational testing period must be communicated to the Contractor, who will then be required to correct the deficiencies. The two (2) week operational testing period will begin again after all deficiencies have been cleared.
 - 5.5.12 Equipment warranty period will start on the date the system is formally accepted.5.6

5.6 Institution Operations

The contractor must take every precaution to minimize any disturbance to institutional operations. Equipment and systems operational down time must be kept to a minimum. All down time must be coordinated with the Assistant Warden Operations on site or designate. The contractor's staff may be required to work during evenings, nights and/or weekends to reduce the amount of down time and to meet operational requirements. The contractor and his staff on site must cooperate fully with operational staff and conform to all security requirements.

5.7 **Institution Address**

Atlantic Institution
13175 Route 8
P.O. Box 102
Renous, New Brunswick
E9E 2E1

Dorchester Penitentiary
4902 Main Street
Dorchester, New Brunswick
E4K 2Y9

Nova Institution
180 James Street
Truro, Nova Scotia
B2N 6R8

Springhill Institution
330 McGee Street
Springhill, Nova Scotia
B0M 1X0

Contact Person - all sites
CESM, Larry Carter NHQ Atlantic
Tel: 906-597-8651 ext 2302

5.8 **Integration Responsibility**

The contractor is responsible for providing a fully functional system

5.9 **Security**

The Contractor must submit completed CPIC forms for all staff who will be working at the Institutions. The CPIC forms must be submitted to the RTEO, or his designate, ten (10) working days prior to the start-up date. (Form 1279-1 included)

5.10 **Schedule**

In accordance with ES/SOW-0101, the contractor must provide a detailed work schedule for the installation activities. This schedule must reflect the complete implementation plan by identifying the nature of the work to be performed and the area affected.

5.11 **Safety**

The Contractor must comply with the document titled "Safety Regulations for Security Electronics Contractors Working at CSC Institutions" attached as Annex B.