OFFICE OF
INFORMATION
AND TECHNOLOGY

# VA IT Equipment Compatibility Standard

*Version 1*

Aug 22, 2023 | Data Center and Infrastructure Engineering (DCIE)

# Table of Contents

**Table of Contents** ..... 1
**1 Introduction** ..... 2
1.1 Purpose ..... 2
1.2 Scope ..... 2
1.2.1 Scope Inclusions ..... 2
1.2.2 Scope Exclusions ..... 4
1.3 Variances and Waivers ..... 5
**2 Constraining Policies, Directives, and Procedures** ..... 6
**3 Background: Overview of the Standard** ..... 7
**4 Equipment Criteria** ..... 8
4.1 Architectural and Physical and Installation Criteria ..... 8
4.2 Power/Electrical Criteria ..... 10
4.3 Cooling Criteria ..... 11
4.4 Telecommunications Criteria ..... 11
**5 Equipment Acquisition** ..... 13
5.1 Procurement Notes for Solicitations ..... 13
5.2 Vendor-Provided Equipment ..... 13
**6 Common Telecommunication Spaces** ..... 14
6.1 Data Centers ..... 14
6.2 Entrance Rooms ..... 14
6.3 Antenna Entrance Rooms ..... 15
6.4 Telecommunications Rooms ..... 15
**7 Configuration Management** ..... 16
7.1 Installation and Rack Elevation Guidance ..... 16
7.2 Data Center Infrastructure Management ..... 16
**Appendix A: Sample IT Hardware Procurement Requirements** ..... 17
**Appendix B: Figures, Tables, & Other References** ..... 25
B.1 Figures ..... 25
B.2 Tables ..... 26
B.3 Definitions ..... 27
B.4 Acronyms ..... 27
B.5 Contributors ..... 32

# 1 Introduction

## 1.1 Purpose

The purpose of this Enterprise Support Standard (ESS) is to define the minimum technical requirements for standardized IT equipment in Department of Veterans Affairs (VA) telecommunications spaces. The minimum requirements and restrictions are necessary to ensure that IT equipment can be installed and operated in the standardized VA telecommunications environment. This ESS is intended to be used in conjunction with other standards including the Infrastructure Standard for Telecommunications Spaces (ISTS) and Local Area Network (LAN) baseline to support consistency of the standardized operating environments. This standard is designed to ensure the safe, secure, and reliable operation of VA IT equipment and infrastructure at the lowest lifecycle cost.

## 1.2 Scope

This document provides an ESS for IT equipment compatibility requirements operating in VA enterprise telecommunications spaces.

### *1.2.1 Scope Inclusions*

This ESS applies to all VA telecommunications spaces including:

- Data centers (aka computer rooms, server rooms, Main Computer Rooms (MCRs), etc.) of all Core Data Center (CDC), Campus Support Center (CSC), Mission Support Center (MSC), and Network Support Center (NSC) classifications
- Telecommunications Rooms (TRs), or deprecated terms no longer used (e.g., Intermediate Distribution Frame (IDFs), network closets, telephone closets, switch rooms, etc.)
- Entrance Rooms (aka demarcs, antenna entrance rooms, or headend rooms, etc.)
- Telephone Equipment Rooms (TERs), telephone rooms, Private Branch Exchange (PBX) rooms, etc.
- Rooms of similar function supporting other VA user groups Facilities Management Service (FMS), Police/Security, Clinical Engineering, etc.
- Leased telecommunications spaces (aka Trusted Internet Connection (TIC) and Gateway collocation facilities)

This ESS applies to the following types of components:

- IT equipment including:
  - All computer hardware serving a centralized support function (see Scope Exclusions below)
  - Servers and virtual server hosts
  - Storage devices (spinning disk hard drives, solid state hard drives, compact disk, and Digital Versatile Disk (DVD) reader/writer equipment, magnetic tape equipment, etc.)
  - Networking equipment (switches, fabric interconnects, fabric extenders, etc.)
  - Converged infrastructure equipment providing multiple functions
  - Distributed Antenna System (DAS) equipment for cellular reinforcement (see Scope Exclusions below)
  - IP-based recording equipment (Network Video Recorders (NVRs), Digital Video Recorders (DVRs), etc.)

This ESS applies to all IT Equipment that will be installed in a VA telecommunications space without regard to ownership or manner of acquisition:

- VA-purchased IT equipment
- VA-leased IT equipment
- Wide Area Network (WAN) carrier circuit vendor-owned equipment
- Vendor-owned IT equipment
- Vendor-managed IT equipment
- IT equipment supporting all VA organizations including but not limited to:
  - Office of Information Technology (OIT)
  - Facility Management Services (FMS)
  - Clinical Engineering (e.g., Biomedical Engineering or Healthcare Technology Management)
  - VA Police/Security
  - VA Research
  - VA Partner Organizations (e.g., local research hospital partners, other federal agencies)

Please note that legacy equipment installed and operational at the time of publication of this standard is grandfathered to not meet these requirements, but that such equipment shall be replaced with compliant equipment and connectivity in the next technology refresh cycle. Lifecycle replacement, refresh, or upgrade of any individual element of an IT equipment system (such as a converged server/storage/networking system) shall trigger the requirement to make the entire system compliant, including, but not necessarily limited to, physical relocation of system elements and replacement of interconnecting network cabling.

### *1.2.2 Scope Exclusions*

The following types of equipment and systems are not subject to the requirements of this ESS:

- End-user IT equipment (workstations, laptops, monitors, and other equipment intended for use at a user's work area)
- Printers, scanners, copiers, etc.
- Point of Sale (PoS) systems, kiosks, etc.
- IT equipment integrated into healthcare equipment systems (e.g., servers as part of a pharmacy dispensing system or workstations providing a function requiring direct attachment to a biomedical system such as an imaging unit for the operator to use the system, etc.)
- Television distribution and legacy camera systems using coaxial cabling
- When designed by the manufacturer to be wall-mounted in a dedicated metal enclosure:
    - Fire protection control systems
    - Access control systems
    - Environmental monitoring and control systems
    - When provided in a 19 in. rack-mountable format and with the ability to communicate over Internet Protocol (IP), these systems will no longer be excluded.

Specific types of High-Performance Computing (HPC) systems may not be required to meet all requirements of this ESS. This includes single- and multiple-cabinet mainframe computing equipment, supercluster computing equipment, and multi-cabinet dedicated storage systems. These types of systems may only be installed in purpose-built VA CDCs and Rating 3 MSCs with special engineering coordination by Data Center and Infrastructure Engineering (DCIE) following confirmation of appropriate physical, electrical, and environmental capabilities at specific facilities.

Radio equipment special systems installed in Antenna Entrance Rooms are strongly encouraged to follow the guidance in this ESS because of the standardized designs of these VA telecommunications spaces. This ESS recognizes that some types of Distributed Antenna System (DAS) equipment is not sized to be installed within the confines of a network rack with 19 in. rails. These types of systems may only be installed in Antenna Entrance Rooms or TRs with unutilized physical space for the installation of an additional enclosure (while maintaining defined 3 ft clearance requirements) and with special engineering coordination by DCIE.

## 1.3 Variances and Waivers

The Authority Having Jurisdiction (AHJ) for this ESS is VA OIT Infrastructure Operations (IO) DCIE. Any deviations from the requirements in this ESS must be approved in writing by the AHJ authority in advance of installation, procurement, or contracting with any party to provide equipment that does not meet these requirements.

Subject to the legacy equipment technical constraints noted below, equipment that does not comply with these requirements will not be allowed to be physically installed or connected to the VA LAN or other networks operating in VA facilities.

Variances or waivers from the requirements of these standards shall be submitted using a Request for Variance following the processes established in Appendix A of the ISTS.

# 2 Constraining Policies, Directives, and Procedures

This ESS complies with the following policies, directives, and procedures:

- Office of Information and Technology Service Delivery and Engineering (SDE) - Medical Device Isolation Architecture (MDIA)
- Public Law 29 U. S. C. 794d: Rehabilitation Act of 1973, Section 508 - IT Accessibility Laws and Policies
- Use of the VA Enterprise Cloud (VAEC) to Host Applications (VA Cloud First Policy) - Memorandum October 29, 2019
- VA Enterprise Architecture (VA EA) - VA EA Release Evolution
- VA Enterprise Privacy Program - VA Directive 6502
- VA Information Security Program - VA Directive 6500 and VA Handbook 6500
- Virtualization and Consolidation of Servers (Server Virtualize First) - VAIQ 7266972
- VA Infrastructure Standard for Telecommunications Spaces (ISTS)
- VA Enterprise LAN Baseline

This ESS is technically constrained by the following:

- Legacy systems and equipment that do not comply with these technical requirements: Legacy system and their designs are grandfathered. Any system that is procured, acquired, leased, or installed in a VA telecommunications space following the effective date of the publication of this standard shall follow the requirements herein and the legacy non-compliant elements of the system shall be removed.
- Legacy VA data centers that do not have passive structured cabling systems installed: As of 2023, VA data centers of the CSC classification at VA Medical Centers (VAMCs) across the enterprise are being modernized to support deployment of an Electronic Healthcare Record (EHR) system intended to replace VA's legacy EHR system, Veterans Integrated System Technology Architecture (VistA). These telecommunications spaces will generally have the passive structured cabling systems in place supporting this ESS following this enterprise modernization effort. The lack of an installed passive structured cabling system in a VA data center does not provide an exclusion from compliance with the requirements of this ESS.

# 3 Background: Overview of the Standard

Telecommunications spaces operated by the Department of Veterans Affairs are transitioning to a standardized, pre-configured model providing IT equipment enclosures, power, heat rejection, and passive structured cabling systems. IT equipment selected for operation in VA facilities must be configured to operate in these standardized data center models without requiring special consideration.

Some types of IT equipment and systems that have been installed in VA telecommunications spaces in the past do not allow the VA's standard telecommunications infrastructure to support them appropriately. Some manufacturers' systems are explicitly designed in such a manner as to not be compatible with the VA telecommunications infrastructure. Systems with these types of elements or characteristics will remain in operation until their next technical refresh but must be replaced with technology that is compliant and compatible. Examples of non-compliant items in some existing systems include:

- Network cabling passing directly between servers in different IT equipment enclosures
- Provision of rack-mounted Uninterruptible Power Supply (UPS) systems for individual IT equipment systems
- Use of Active Optical Network (AON) cabling between server/storage and networking elements
- Equipment airflow rear-to-front and not configurable/reversible

This ESS provides the minimum requirements for standardized IT equipment that will utilize the enclosures, power distribution, cooling systems, and passive structured cabling systems in VA telecommunications spaces. Adherence to this standard will ensure the safe, secure, and reliable operation of VA IT equipment and infrastructure. The VA will periodically review and update this standard to reflect the latest technology and industry best practices.

Where clarification of requirements is necessary, refer to the ISTS or contact DCIE, directly.

# 4 Equipment Criteria

IT Equipment in the VA environment shall comply with all the requirements of the elements below.

## 4.1 Architectural and Physical and Installation Criteria

1. Use Electronic Industries Alliance (EIA)-310 compliant 19 in. rack-mountable form factor.
2. Provided with static rails. The rails shall be industry standard square hole, toolless, and provide the ability for a single person to install and remove the IT Equipment (subject to two-person lift weight restrictions). For form factors larger than 1 Rack Unit (RU), the rails shall be ball bearing.
3. All IT Equipment shall be installed in a VA-provided standardized IT equipment enclosure (e.g., server cabinet, network channel rack, network cabinet, or telecommunications enclosure).
    a. No server/storage equipment may be installed/operated in a network rack/cabinet.
    b. Exception: Configuration of emergency systems requiring 4-hour battery backup. These systems should be wall-mounted rather than rack-mounted to avoid potential issues with cascaded UPS systems powering the equipment. Typically, these types of systems will use a dedicated wall-mounted enclosure with battery equipment rather than a Commercial Off the Shelf (COTS) rack-mounted UPS system.
4. Recommendation, not required:
    a. Power Supply Units (PSUs) on the hardware chassis should be on the left and right sides, not both on the same side (upstream power sources are located on the left and right sides of the enclosure) where power cords will need to be of differing lengths and one side strung across to the opposite side of the enclosure. An example of this is shown in Figure 1 below. While this installation does not meet all other VA standards requirements (for example for differentiated colors for A/B power cords), observe that the exhaust of the IT equipment is not blocked, allowing for effective rejection of heated exhaust air.

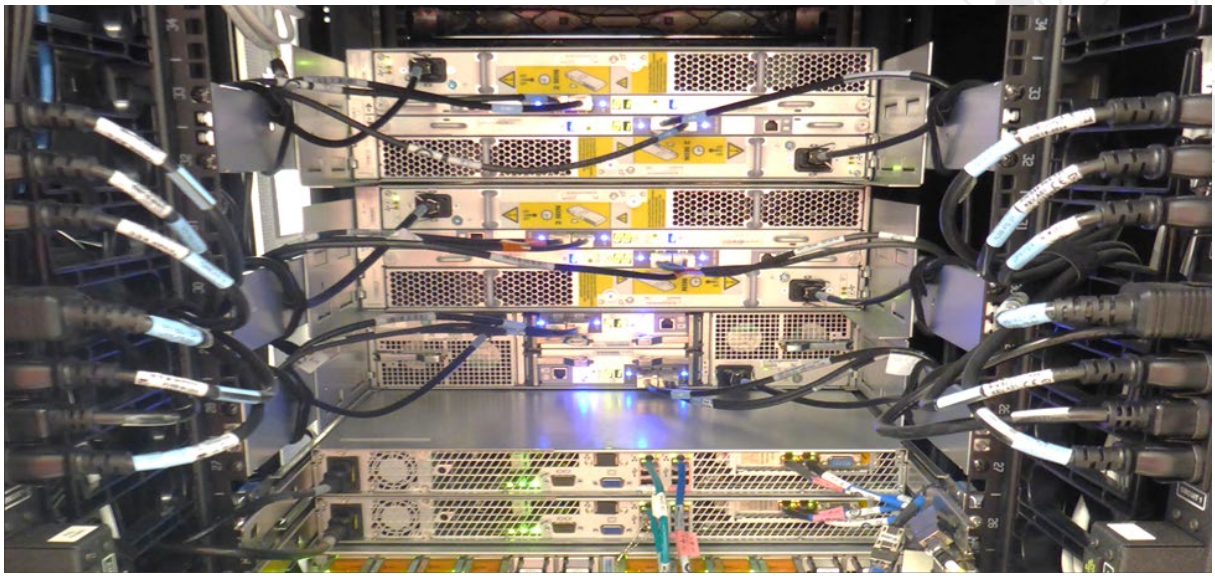

*Figure 1: Server Cabinet with Power Distribution Units on Both Sides of Chassis*

b. Network Interface Cards (NICs) on the hardware chassis should be on the left and right sides, not both on the same side; (Equipment Distributor and other fiber/copper patch equipment are located on the left and right sides of the enclosure) where patch cables will need to be of differing lengths and one side strung across to the opposite side of the enclosure.

c. If these recommendations are not met, horizontal cable management for power and telecommunications will be required to be provided with the hardware and installed on the rear rack rails of the enclosure. An example of this is shown for fiber and copper horizontal cable management in Figure 2 below:

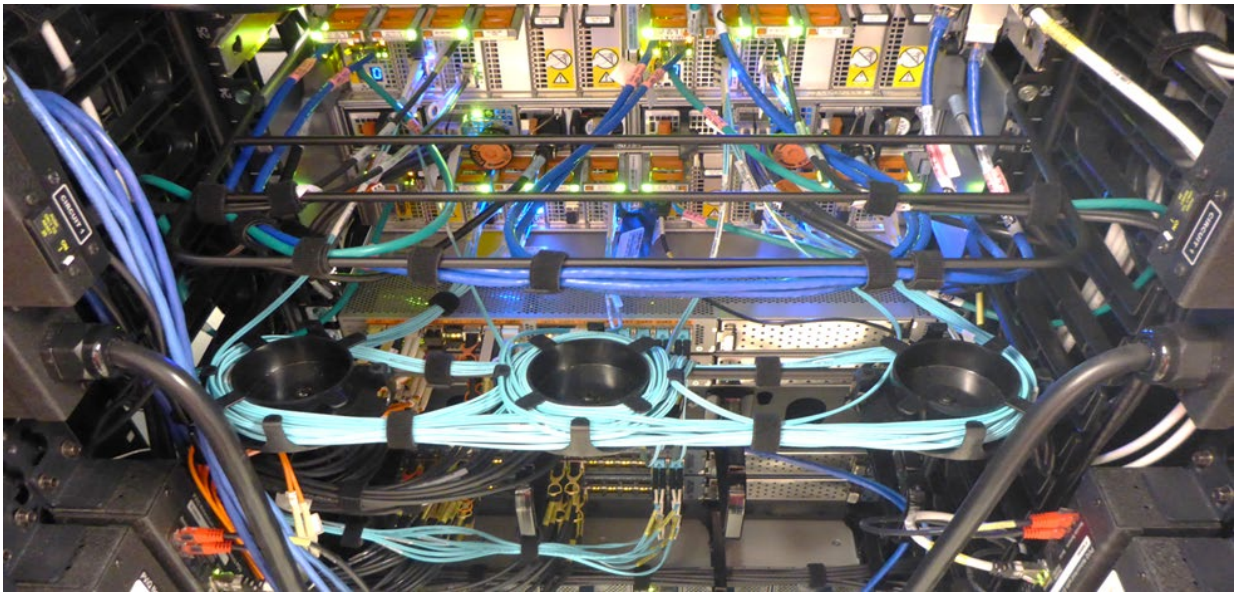

*Figure 2: Fiber and Copper Horizontal Cable Management Example*

## 4.2 Power/Electrical Criteria

1. IT Equipment shall be Energy Star certified to minimize energy consumption.
2. Equipment intended to be located in a data center environment shall be capable of using 208 V power (120 V single-phase-only equipment not acceptable).
    a. Equipment intended to be located in a distributed telecommunications space environment shall be provided with PSUs capable of using 208 V power distribution (distributed telecommunications spaces are the TRs, Entrance Rooms, and Antenna Entrance Rooms, as opposed to the campus centralized telecommunications space, the data center).
    b. Equipment intended to be located in a Telecommunications Enclosure (TE) environment shall be provided with PSUs capable of using 120 V single-phase power distribution.
3. Equipment shall be provided with matching dual hot-swappable PSUs. Equipment incapable of being provided with dual PSUs shall be provided with micro-Automatic Transfer Switch (ATS) equipment (see DCIE *White Paper: IT Equipment Automatic Transfer Switches (ATS)*).
4. Equipment shall be provided with IEC 60320 power cords, one black and the other white/gray (or other distinguishable color). NEMA 5-15 power cords will be provided for 120 V-only equipment to be installed in a TE environment.
5. VA telecommunications environments provide for 5 kW Standard Density IT equipment enclosures. The total power consumption of all devices in a Standard Density enclosure may not exceed 5 kW.
    a. The total power consumption of all devices in a Standard Density enclosure in a legacy VA data center environment (using underfloor cooling air distribution) may not exceed 3.5 kW.
    b. The power consumption of IT equipment may be estimated by vendor-provided test information for a given configuration.
    c. The PSU rating is not equivalent to the power consumption of the equipment.
    d. If vendor power consumption information is not available, assume that the amount of power consumed will be equivalent to 40 % of the wattage rating for one of the dual redundant PSUs. Extensive testing of a variety of IT equipment across VA has shown that the mean power consumption of IT equipment does not exceed 25 %, with a distribution approximated by the following histogram. The 40 % factor is deemed to be sufficiently conservative for design purposes, and operational checks will detect any consumption that exceeds these limits for correction. See Figure 3 below:

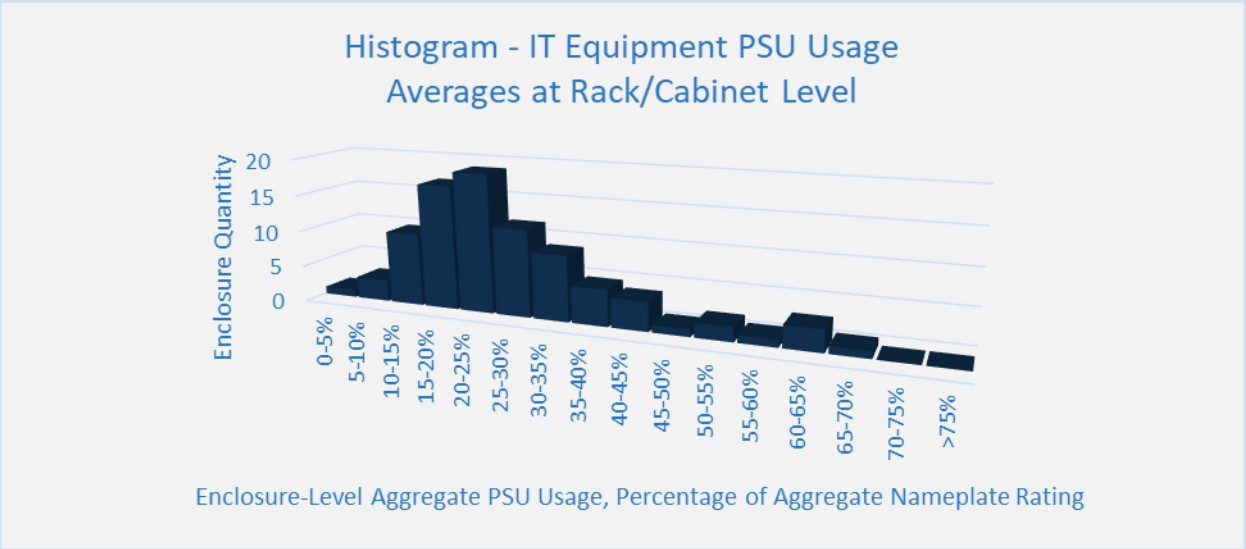


*Figure 3: IT Equipment PSU Usage*

6. Dedicated UPS equipment may not be specified or provided for the IT equipment. VA telecommunications environments are already provided with room- or rack-level UPS equipment for the maximal power consumption at the rack level.
7. IT equipment shall be provided with 6 AWG equipment bonding conductors appropriate to the type of device (server/storage or networking) with the appropriate hardware to connect to the rack bonding busbar or the rack bonding conductor.

## 4.3 Cooling Criteria

1. Airflow is required to match the front-to-rear (typically front-to-vertical-exhaust-duct) alignment of VA heat rejection systems design.
2. Network equipment (e.g., switches, fabric interconnects, fabric extenders, etc.) may be provided with user-configurable airflow systems (front-to-rear and rear-to-front) but shall not be designed for installation and use only in a rear-to-front configuration.

## 4.4 Telecommunications Criteria

1. IT Equipment shall be compliant with Federal Information Processing Standards (FIPS) 140-2 security requirements.
2. Communications between the network and the IT equipment must use VA-provided passive structured cabling system (OM4/5 or Cat 6A).
3. The IT equipment shall not have active cabling (e.g., Direct-Attached Cabling (DAC), Active Optical Cabling (AOC), etc.) connectivity requirements except to interconnect server/storage equipment within the same enclosure.
4. IT equipment shall use VA-provided LAN switches for connectivity to the network.

5. Dedicated switches shall not be provided with server/storage equipment or as part of a system. However, fabric extenders and/or fabric interconnects may be provided and placed in dedicated network areas.
6. No switches, fabric extenders, fabric interconnects, or similar networking equipment may be placed in a server cabinet.

# 5 Equipment Acquisition

## 5.1 Procurement Notes for Solicitations

Requirements of this standard shall be provided to all IT equipment providers as part of any procurement, acquisition, managed services, or similar contract vehicle that intends to provide active IT equipment (server, storage, networking equipment) for installation in VA telecommunications spaces.

Note: DCIE strongly recommends that this standard be included as an appendix to each contract to prevent equipment being provided that will not operate properly in the standardized VA telecommunications environments.

## 5.2 Vendor-Provided Equipment

Vendor-provided IT equipment enclosures, power distribution equipment, UPS, and other equipment already provided in the VA standardized data center model are prohibited and shall not be specified, provided, or installed in the VA telecommunications space environment.

# 6 Common Telecommunication Spaces

IT Equipment shall only be installed in the appropriate standardized VA telecommunications environments that are purposefully built to properly house, operate, and maintain VA IT equipment as intended and specified in the ISTS.

There are four general classifications of telecommunications space:

- Data Centers
- Entrance Rooms
- Antenna Entrance Rooms
- Telecommunications Rooms

IT equipment shall not be planned to be installed in a space that does not meet one of the classifications listed above.

In some (typically smaller) types of VA facilities, the space classifications present in a VA facility may be combined.

## 6.1 Data Centers

Data Centers are the buildings or portions of a building whose primary function is to house a computer room and its support areas. The computer room is the space whose primary function is to accommodate data processing equipment.

There are four classifications of data centers in the VA architecture. In the context of this Standard, data centers requiring configuration management coordination for equipment installation planning are limited to enterprise CDCs, VA medical center CSCs, and MSCs. Network Support Center (NSC) data center classifications generally support smaller, less complex, and administratively oriented or small outpatient clinic facilities where the VA has determined that the resources to maintain complete configuration management, are not available.

## 6.2 Entrance Rooms

Entrance Rooms are (typically distributed) telecommunications spaces where the joining of inter- or intra-building telecommunications cabling takes place. In the VA environment, these are typically the locations where demarcation between the telecommunications carrier and VA take place, containing active carrier equipment (routers and similar) and active VA equipment (multiplexers, protocol translation systems, and similar). VA routers are to be located in the MDAs in the data center, not in Entrance Rooms.

## 6.3 Antenna Entrance Rooms

Antenna Entrance Rooms are distributed telecommunications spaces where telecommunications communications that do not use physical media enter VA facilities. In the VA environment, most mission critical campuses have an Antenna Entrance Room where (typically radio frequency) telecommunications signals are transmitted and received, generally located in a rooftop penthouse location at the top of the building. The typical types of equipment found in these spaces include police and fire radio systems, inter-agency communications systems, and cellular reinforcement systems.

Not all VA facilities require or have Antenna Entrance Rooms.

## 6.4 Telecommunications Rooms

Telecommunications Rooms (TR) provide a connection point between backbone cabling (from the data center) and horizontal cabling (to the end-user work area outlet) for a serving zone. Individual floors in VA buildings are broken up into serving zones based on path length restrictions for horizontal cabling media and the maximum density of end-user work area outlets being supported from TR spaces of certain sizes. In the VA environment, these locations contain access switches for the VA LAN, as well as communications interface equipment that supports other users' functions in the serving zone (e.g., fire control panels, access control system controls, nurse call and telemetry system aggregators, and similar).

# 7 Configuration Management

Planning and installation of IT equipment in the three larger VA data center environments (as described above) shall be coordinated for Configuration Management (CM) purposes.

## 7.1 Installation and Rack Elevation Guidance

Installation and rack elevation guidance or distributed telecommunications spaces is covered in supplemental guidance to the ISTS (see the *VA Telecommunications Rack Elevation Usage* white paper for additional information).

## 7.2 Data Center Infrastructure Management

VA maintains a Data Center Infrastructure Management (DCIM) software tool that provides configuration management information on VA data centers and the IT Equipment installed therein. All equipment deployments to the VA data center environment shall be coordinated between the local End User Services (EUS) team and the IO DCIM Team.

# Appendix A: Sample IT Hardware Procurement Requirements

IT hardware procured by VA for installation in VA telecommunications spaces must be compliant with the requirements of the ESS to be able to be operated successfully. This applies equally to VA-owned, contractor-provided, managed services, and similar equipment.

The following list of requirements is an example provided to assist VA requirements developers and contracting office staff with ensuring that they are specifying equipment that is both compliant and will meet the performance expectations of the VA. This requirements list is an example model used by the Data Center Engineering Platforms team to procure enterprise-class server hardware that is compliant with the requirements of the ESS.

The use of this or any similar list is recommended to ensure that VA's technical requirements and limitations are described appropriately to vendors and other supporting contractors.

**List IT Hardware Procurement Requirements**

The Contractor shall provide servers that meet the following requirements, at time of base or option award:

1. Hardware End of Life date + 24 months.
2. Hardware End of Support date + 60 months.
3. All solutions shall be enterprise grade products providing mission critical, 4-hour 24 x 7 support to continental United States and Next Business Day (NBD) support for Alaska, Hawaii, San Juan, US Virgin Islands, Guam, and Manila. Support must be provided by an Original Equipment Manufacturer (OEM) authorized/certified technician(s).
4. Vendor will provide a usable, minimum configuration as required by VA. The proposed server must be certified by the specific OEM to function. No additional hardware, software licensing and/or services will be required for function.
5. The VA may customize components and quantities as needed for workload. For components that are not compatible with each other (i.e., sockets, chassis size, memory configuration) the vendor is responsible for notifying VA and suggesting corrections before award and shipment to VA. VA shall not be responsible for correcting an incompatible order that has been delivered to VA.
6. Vendor server lifecycle changes are common during multi-year contracts. The vendor shall propose recommended changes only if advantageous to government to include increased security, compatibility, or performance. Changes must be accepted by VA. All proposed components and/or servers shall be the same OEM as originally provided (minus subcomponents: memory, interface cards, or adapters).
7. VA is aware next generation technology offerings may not match current Random Access Memory (RAM), disk, etc. quantities or multipliers. The VA will consider changes in technologies that differ from VA requirements, VA will be notified of changes required to

support the new technology offering (i.e., Dual In-line Memory Module (DIMM) change to 24 Gigabyte (GB) RAM requires changes in RAM capacity to 96 GB, 192 GB, 384 GB).

8. Server should be provided with all components, modules, power supplies, cabling, management software and/or licensing required to bring the system online ready to accept VA provided operating system image.
9. System warranty shall include any included software components for hardware or management. If VA has an existing hardware and/or software support agreement, the initial year pricing for this support shall not be included in the overall system cost.
10. Year 1 of hardware/software maintenance for all included components shall be included with the initial purchase/execution of the system option.
11. All data storage components must include 'Keep Your Hard Drive' entitlement, which means that at no time may a data drive leave VA premises for repair and/or replacement. This includes spinning disks, flash type storage devices (e.g., Peripheral Component Interconnect Express (PCIE) 4 and Serial Advanced Technology Attachment (SATA)/Serial Attached Small Computer System Interface (SCSI) (SAS) bus connected), persistent memory, and flash removable media (Secure Digital (SD), Universal Serial Bus (USB) devices).
12. All components shall in no-way limit support of zero-day security patch remediation. This includes hardware and software components. Zero-day patching includes workaround and other manual remediation, vendor shall not provide patching assistance but, if necessary, shall troubleshoot remediation.
13. Provided server shall comply with National Institute of Standards and Technology (NIST) SP 800-193 Platform Firmware Resiliency Guidelines, NIST SP 800-147 BIOS Protection Guidelines, NIST SP 800-147B, Basic Input/Output System (BIOS) Protection Guidelines for Servers.
14. At no time will manufacturer firmware or subcomponent firmware be developed, sourced, or provided by the following countries: Cuba, Iran, Syria, North Korea, Russia, Crimea region of Ukraine, People's Republic of China, Venezuela; or any country that is prohibited from export of U.S cryptography modules; or restricted imports, export, reexport or materiel modifications with information technology, cryptography components. Countries included in the Wassenaar Arrangement (WA) are generally not included in these restrictions, with the exception of Russia and other countries not identified as country group A:1 exempt in Export Administration Regulations (EAR) Supplement No. 1 to Part 740.
15. Provided firmware and software shall be cryptographically signed, using the latest version available at time of assembly. All systems much be configured in Unified Extensible Firmware Interface (UEFI) mode with secure boot enabled by default.
16. During system support process or troubleshooting, network traces, kernel and/or memory dumps shall not be provided outside of United States of America located OE support personnel.
17. System shall include out of band management function to include secure web interface allowing system setting configuration changes, system firmware and subcomponent

firmware updates, disk and volume configuration, inventory, remote console access, virtual media mounting and virtual flash read/write capabilities, network interface configuration and/or monitoring. The out of band management function shall not require additional licensing and will be licensed for the lifecycle of the hardware. The system shall also allow Secure Shell (SSH) access, with standardized access available via Intelligent Platform Management Interface (IPMI), Command Line Interface (CLI). The out of band management shall be secure and able to be configured to the Defense Information Systems Agency (DISA) Security Requirements Guide (SRG) or system management. The out of band management interface shall be configurable to connect to public internet resources for firmware, inventory reporting or any other function.

18. Each system shall include all licensing required to centralize management for policy, configuration, firmware, and monitoring to include remote console access. System shall support monitoring of configuration policies and security posture of the system. The centralized management console shall support log and bundle gathering as needed for technical support. The centralized management console shall support automated vendor ticket creation for hardware component failure and replacement. The centralized management function shall scale to no less than 8,000 instances. No additional licensing and or software components shall be required to fully management systems. The centralized management product shall be configurable to DISA Security Technical Implementation Guide (STIG) requirements, to include integration with VA active directory and two-factor authentication. The centralized management software shall be fully hosted on-premises to VA without any interconnection with public internet resources.
19. Original Equipment Manufacturer (OEM) firmware and/or software updates for components shall be accessible without additional licensing or cost to VA. The updates shall remain available to VA through the entire lifecycle of the provided server and components.
20. System shall provide a dedicated out of band management interface. This management interface shall be 1 GB Base-T. The out of band management interface shall include all licensing required.
21. If additional network interface cards are provided and if the vendor can share the ethernet interface with the Intelligent Platform Management Interface (IPMI), the vendor shall provide these cards if multiple cards are available (i.e., card model 1 is capable of shared IPMI, card model 2 is not capable of shared IPMI. Vendor shall provide card model 1).
22. All provided processors shall support base all-core speeds of at least 2.7 Gigahertz (GHz). All cores on provided socket shall support increasing speeds to at least 3.0 GHz across all sockets simultaneously. Single-core speeds (commonly referred to industry as 'turbo' shall increase to no less than 3.4 GHz on a single core.
23. Included memory shall be compatible with proposed Computer Processing Unit (CPU) and CPU quantity, while meeting industry best practices for high performance computing. Memory speed shall meet or exceed required of provided CPU. Memory shall be of a balanced configuration, distributed equally with identical size and configuration across all sockets. All memory shall be Error Correction Code (ECC) memory modules.

24. System shall have CPU full error correction capability or equivalent. Additionally, shall have ECC ability.
25. Provided memory DIMM sizing and ranking shall provide a balanced configuration while providing the highest available bandwidth and retaining available DIMM slots/channels as possible, at least cost to VA.
26. System per-core mid-level (level 2 or L2) cache shall be at least 1.0MB per core. System per-core last level cache (level 3 or L3) shall be at least 1.375 MB per core, shared. Alternatively, if the processor does not meet the L2 cache ratio requirements; the system shall provide at least 512 Kilobyte (KB) per-core mid-level cache and at least 8.0 MB per core of last level cache. System per-core mid-level (level 2 or L2) cache shall be at least 1.
27. System processor shall support hyper-threading. Logical cores shall not be considered in the VA provided core specification.
28. System shall be capable of supporting Persistent Memory (PMEM). The system shall fully support memory mode or mixed mode configurations. Persistent memory configuration shall comply with industry best practice and provided system limitations.
29. System provided shall be an x86/x64 instruction set based system.
30. System provided shall support hardware assisted virtualization, hardware enforced Data Execution Prevention (DEP).
31. System shall be native UEFI and fully support UEFI security to include Secure Boot. The system shall support legacy boot or BIOS mode. UEFI should be configured as default out of the box configuration.
32. System shall include a Trusted Platform Module (TPM) v2.0 hardware module. This module must be Federal Information Processing Standard (FIPS) 140-2, if different, and be a separate replaceable module on the motherboard and cannot be integrated (non-replaceable).
33. System processors shall include hardware remediation of known CPU vulnerabilities to include Spectre, SpectreNG, SpectreRSB, Meltdown, L1TF, Store-to-leak Forwarding, ZombieLoad, Fallout, and RIDL.
34. System shall support Generation 4 PCIE for all platforms.
35. For all 2 socket or higher systems, the systems shall support the installation of at least two Nonvolatile Memory Express (NVMe) PCIE 4 devices, population is outside of scope of this specification.
36. For all 2 socket or higher systems, the systems shall support the installation of at least two full length graphics acceleration devices of at least 48 GB RAM or 32 GB RAM shared Graphics Processing Unit (GPU) platform; population is outside of scope of this specification.
37. System shall be provided with at least two power supply units with fully automated and automatic redundancy to protect the system from power supply and/or power source failure. Power Supply sizing shall allow the system to function with half of the power

supplies available, while providing the lowest quantity power usage required. If the system requires more than two power supplies, power supply and provided cable quantity shall be provided.

38. Power supplies must be EnergyStar certified and Electronic Product Environmental Assessment Tool (EPEAT) Bronze certified. Power supplies shall support active state power management, reducing supply as needed to maintain system function while using the minimum source power required. Due to delay in EnergyStar and EPEAT certification process, VA will accept documentation of server submission to EnergyStar and EPEAT.
39. System shall provide at least two USB 3.0 ports, and one USB 2.0 port or higher, alternatively USB-C ports can be provided. These ports shall be fully configurable to include disablement or limiting interface to human interface device types only.
40. System shall provide a Recommended Standard 232 (RS-232) serial port interface, this interface can be either Registered Jack-45 (RJ45) or DB-9. This port shall be fully configurable to include disablement.
41. System shall provide DB15 Video Graphics Adapter (VGA) video connector. This port shall be fully configurable to include disablement.
42. All external interface ports to include USB, Serial or Video shall include the ability to be disabled.
43. The server form factor shall be at minimum 1 RU. The server provided shall meet minimum VA requirements. If vendor requires due to VA optional components, the server shall be increased to 2 RU to 4 RU - while meeting all other VA requirements. The VA shall be informed if a larger server is required. The VA should be provided the smallest form factor to meet requirements.
44. The server shall be provided with static rails for standard 1 RU servers. The rails shall be industry standard square hole, toolless and provide the ability for a single person to install and remove a server. For 2 RU to 4 RU form factors, the rails shall be ball bearing.
45. The server is not required to be provided with cable management arms or paper documentation.
46. The server shall have automatic fault alerting by external visible light.
47. The server shall have a permanent serial number placement, visible on the front and back of the server. The serial number may be affixed via a plastic tab or similar that is not an obvious placement.
48. The server shall include a physical power button on the front of the server. The power button shall be able to be disabled via configuration.
49. The server shall be provided with one CPU socket populated, as specified by VA. The specified memory configuration shall be populated to support single socket. If the VA chooses, the server shall be configured with two or four identical CPUs. The relevant form factor, memory/DIMM configuration and or relevant add-on modules shall be adjusted to comply with OE requirements for multiple socket configuration. If additional or different

power supplies are required for change in chassis and/or power load of multiple CPUs, then they shall be provided as needed.

50. The system shall be provided with 10 physical cores per CPU. If the VA chooses, the per-CPU core count shall be at least 16, 24, or 28 cores. If a processor exceeds core count requirements, it shall be acceptable if it meets all other VA requirements. As cores increase, mid-level and last level cache should be increased proportionally. Logical cores (hyper-threads) are not included in this core count.
51. The system shall be provided with at least 64 GB RAM. If 64 GB is not a proper, balanced memory configuration, additional memory should be provided to meet OE requirements. The memory should be balanced across all populated sockets as necessary. If the VA chooses, the server shall be populated with 64, 96, 128, 192, 256, 384, 512, 768, 1024, 1152, 1536, 2048, or 2304 GB memory. The configuration shall also include appropriate changes to CPU specification to support necessary per-socket memory limitation.
52. The system shall be provided with zero persistent memory per socket. If VA chooses, the server shall be populated with 128, 256, 512 GB persistent memory PER SOCKET to match industry best practices. The persistent memory configuration shall be of correct ratio to volatile memory as required by industry.
53. The system shall be provided with a boot disk controller. This controller shall either be software or hardware Redundant Arrays of Independent Disks (RAID) to support disk mirroring of provided boot disks. The boot disk controller does not need to meet VA encryption requirements; encryption if available, shall be provided. The disk controller shall support automatic failure reporting and recovery as needed for disk failure or pending failure.
54. The system shall be provided with two identical boot disks of at least 240 GB usable capacity in a mirror or RAID 1 configuration. The boot disk shall be non-volatile solid-state flash, no spinning disk or moving components shall be provided. The boot disk flash type shall meet industry best practices for performance with 1 drive write per day. The boot disks shall be fully supported by hypervisor or server operating system vendors to include Microsoft Windows Server 2022 and RedHat Enterprise Linux 8. If the VA chooses, the boot disk usable capacity shall be at least 480 GB.
55. The system shall be provided with a 'Data Drive' RAID or SAS pass thru controller only if specified. If VA chooses, the system shall be provided with a RAID controller with flash backed write cache or SAS controller host bus with internal Just a Bunch of Disks (JBOD) or pass-through support. The provided storage controller shall meet industry best practices.
56. The optional RAID controller shall support any mix of RAID 0, 1, 5, 6, 10, 50, 60 or JBOD mode. The RAID controller shall support at least 10 RAID groups or virtual volumes. The RAID controller shall support fully automated failure reporting and rebuilding to configured RAID level.
57. The optional RAID or SAS Host Bus Adapter (HBA) controller shall support FIPS 140-2 volume encryption, to include key changes, un-encryption, and re-encryption. The encryption

process shall not provide overhead to the system performance. The VA will not provide a key management server for the system, the system must be able to store keys in TPM or RAID controller itself without risk of key loss. If necessary, the provided disks must be of Self Encrypting Drive (SED) type, this is only required if the RAID controller does not meet VA encryption requirements.

58. Either combination of SED or controller encryption is acceptable if it meets intended VA requirements of encryption at rest/transit. The encryption requirement does not apply to the boot device and boot device controller. The VA will not accept third-party software encryption or guest operating system-based encryption.
59. The system shall be provided with data drives only if specified AND appropriate disk controller is selected. The VA shall specify a usable drive capacity of at least RAID 5 3.5, 5, 8, 12, 20, 50, 100, or 150 Terabyte (TB) accounting for a single like configured hot spare. The VA will likely choose to use a different volume RAID configuration, but for this calculation a spare and RAID 5 is assumed - even if a SAS HBA is selected the same calculation shall apply (one hot spare). All disks and controllers shall be cabled or use extenders as necessary to meet VA requirements.
60. All data drives will be non-volatile solid state or flash disks, with appropriate internal coding to allow wear leveling and redundancy. The provided disks shall support an average of 3x drive writes per day.
61. The server platform provided shall include at least six disk slots. If additional slots are needed to meet usable data disk capacity requirement, vendor will provide platform with necessary disk slots to meet requirement.
62. The system shall be provided with at least two 1/10 Gigabit Ethernet (GbE) base-T interfaces.
63. If VA chooses, the system shall be provided with a combination of up to two interface cards with at least the following interfaces 2x 10/25 GbE Small Form-factor Pluggable, SFP28, 2x 1/10 GbE Base-T, 2x 40/100 GbE Quad Small Form-factor Pluggable, QSFP28. Any necessary modules shall be provided with the interface cards. The optional network interfaces shall support, RDMA, Multi-VLAN capability, VXLAN (eVPN), with up to 4,096 VLAN support to include pruning, native/default VLAN with the port aggregation technologies.
64. If VA chooses, the system shall be provided with one or two storage interface cards with at least the following interfaces 2x 16 GB Fibre Channel, 2x 32 GB Fibre Channel. Any necessary modules shall be provided with the interface cards.
65. The system shall be provided with quantity of necessary power cables to match power supply quantity. The supplied power cables shall be 1 m or shorter C13-C14, one black and one white/gray (or other distinguishable color). Power cable connector shall match server inlet requirement.
66. If VA chooses, installation services shall be provided with the system. The vendor will coordinate basic rack and stack of the server hardware, power cabling, network, or storage

interface cabling, and configure the out of band management address. The VA shall be provided with the username/password at time of configuration.

67. Due to the variation of VA facilities and infrastructure configurations across the VA, modules and cabling requirements vary significantly. Each server shall be provided with at least three Cat 6A patch cords per. The patch cords length will be selectable with a default of 3 m.
68. Optionally, for SFP28, QSFP28 and Fibre Channel connectivity, VA shall specify quantity of 2, 4, 6, 8, or 10 OM4 Lucent Connector (LC)/LC aqua multi-mode fiber cables.
69. Vendor shall provide access to computer-based training modules for basic server functions to include installation, maintenance, troubleshooting, configuration, out of band management, and centralized management.

# Appendix B: Figures, Tables, & Other References

## B.1 Figures

*Figure 1: Server Cabinet with PDUs on Both Sides of Chassis* ..... 9

*Figure 2: Fiber and Copper Horizontal Cable Management Example* ..... 9

*Figure 3: IT Equipment PSU Usage* ..... 11

## B.2 Tables

*Table 1: Acronyms*.....27

*Table 2: Contributors*.....32

## B.3 Definitions

**IT Equipment:** Systems that communicate using Internet Protocol (IP) traffic over a network of fiber optic and twisted pair copper, with a primary function related to the collection, transfer, storage, and/or processing of data.

**Data Processing Equipment:** Electrically operated equipment that accumulates, processes, and stores data.

**Structured Cabling:** A complete system of cabling and associated passive hardware which provides a comprehensive telecommunications infrastructure allowing IT equipment connected to it to communicate.

## B.4 Acronyms

For other acronyms and initialisms, VA employees and contractors with VA intranet access may refer to the full VA Acronym List. All others may inquire with Enterprise Data Center and Infrastructure Engineering (DCIE) at VAITESEDatacenterEngineering2@va.gov.

*Table 1: Acronyms*

| Acronym | Definition |
|---|---|
| AHJ | Authority Having Jurisdiction |
| AOC | Active Optical Cabling |
| AON | Active Optical Networking |
| ATS | Automatic Transfer Switch |
| AWG | American Wire Gauge |
| BIOS | Basic Input/Output System |
| Cat 6A | Category 6A copper Unshielded Twisted Pair (UTP) cabling |
| CDC | Core Data Center |
| CLI | Command Line Interface |
| CM | Configuration Management |
| COTS | Commercial Off the Shelf |

| Acronym | Definition |
|---|---|
| CPU | Central Processing Unit |
| CSC | Campus Support Center |
| DAC | Direct-Attached Cabling or Direct Attached Copper |
| DCIM | Data Center Infrastructure Management |
| DIMM | Dual In-line Memory Module |
| DISA | Defense Information Systems Agency |
| EAR | Export Administration Regulations |
| ECC | Error Correction Code |
| EHR | Electronic Health Record |
| EIA | Electronic Industries Alliance |
| EPEAT | Electronic Product Environmental Assessment Tool |
| ESS | Enterprise Support Standard |
| EUS | End User Services |
| FIPS | Federal Information Processing Standard |
| FMS | Facilities Management Service |
| GB | Gigabyte |
| GbE | Gigabit Ethernet |
| GHz | Gigahertz |
| GPU | Graphics Processing Unit |
| HBA | Host Bus Adapter |
| HPC | High Performance Computing |

| Acronym | Definition |
|---|---|
| IDF | Intermediate Distribution Frame (archaic) |
| IO | Infrastructure Operations |
| IPMI | Intelligent Platform Management Interface |
| ISTS | Infrastructure Standard for Telecommunications Spaces |
| JBOD | Just a Bunch of Disks |
| KB | Kilobyte |
| LAN | Local Area Network |
| LC | Lucent Connector |
| MCR | Main Computer Room |
| MSC | Mission Support Center |
| NBD | Next Business Day |
| NIC | Network Interface Card |
| NIST | National Institute of Standards and Technology |
| NSC | Network Support Center |
| NVMe | Nonvolatile Memory Express |
| OEM | Original Equipment Manufacturer |
| OIT | Office of Information Technology |
| OM4 | Optical Multimode 4 multi-mode fiber optic cabling |
| PBX | Private Branch Exchange |
| PCIE | Peripheral Component Interconnect Express |
| PMEM | Persistent Memory |

| Acronym | Definition |
|---|---|
| PSU | Power Supply Unit |
| QSFP | Quad Small Form-factor Pluggable |
| RAID | Redundant Array of Independent Disks |
| RAM | Random Access Memory |
| RJ | Registered Jack |
| RU | Rack Unit |
| RS | Recommended Standard |
| SAS | Serial Attached SCSI |
| SATA | Serial Advanced Technology Attachment |
| SCSI | Small Computer System Interface |
| SD | Secure Digital |
| SFP | Small Form-factor Pluggable |
| SRG | Security Requirements Guide |
| SSH | Secure Shell |
| STIG | Security Technical Implementation Guide |
| TB | Terabyte |
| TPM | Trusted Platform Module |
| TR | Telecommunications Room |
| TIC | Trusted Internet Connection |
| UEFI | Unified Extensible Firmware Interface |
| UPS | Uninterruptible Power Supply |

| Acronym | Definition |
|---|---|
| USB | Universal Serial Bus |
| UTP | Unshielded Twisted Pair |
| VA | Veterans Affairs |
| VGA | Video Graphics Adapter |
| VistA | Veterans Integrated System Technology Architecture |
| WA | Wassenaar Arrangement |
| WAN | Wide Area Network |

## B.5 Contributors

Contributors to the development of this document are as follows:

*Table 2: Contributors*

| Name | Office | Role |
|---|---|---|
| Michael Julian | Office of Information and Technology (OIT), Infrastructure Operations (IO), Application Hosting, Cloud, and Edge Solutions (ACES) (OIT IO ACES, Data Center and Infrastructure Engineering (DCIE) | SME, Team Leader, Telecommunications Distribution Design, Original ISTS Standard Author |
| Kelly Bates | OIT IO ACES DCIE | SME, Electrical and Mechanical Design |
| Kevin Grzelka | OIT IO ACES DCIE | SME, Telecommunications Space Design, ISTS Design Template Author and Custodian |
| John Wernau | OIT IO ACES DCIE | SME, Energy Efficiency and Airflow Design, ISTS Standard Custodian |
| Glenn Porter | Bob David Rowe (BDR) Solutions, LLC | Program Manager |
| Tim Draper | BDR | QA Manager |
| Matthew Shaffer | BDR | Functional Area Expert II |
| Christopher Martin | BDR | Functional Area Expert II |
| Aditya Chebolu | BDR | Technical Writing, CommonLook Office |