# IT Shared Services Standard: Hyper Converged Infrastructure System

For South Carolina State Agencies
Version 1.0

Effective: October 2, 2018

admin
THE SOUTH CAROLINA
DEPARTMENT *of* ADMINISTRATION

# Revision History:

| Date | Author | Title | Ver. | Notes |
|---|---|---|---|---|
| 10.02.2018 | Security and Architecture Review Board | Standards | 1.0 | Recommended by the SARB Subgroup. Standard finalized. |

# Table of Contents


Revision History: ..... 2
Rationale ..... 4
Agency Exception Requests ..... 4
Business Need ..... 4
Product Description ..... 4
Expected Benefits ..... 5
Purchasing ..... 5
Maintenance ..... 5
Training ..... 6
Technical Requirements ..... 7
Technology Adoption ..... 10
Emerging Technologies ..... 10
Strategic Technologies ..... 10
Contained Technologies ..... 11
Obsolescent/Rejected Technologies ..... 11
Appendix A ..... 12

## Rationale

Information Technology departments are increasingly being seen as service delivery centers for business. Demands upon IT departments are increasingly faced with the need to rapidly respond to business needs with ever greater calls for self-service portals, system availability and greater data security. This evolution has led to widespread adoption of cloud technologies, but not all data sets or applications can move to commercial cloud service providers. Therefore, business units, particularly in the government space, have begun to adopt hyperconverged computing environments as a way of building virtual private cloud computing within their own facilities.

This document sets out the technology requirements for hyperconverged computing within the State of South Carolina's enterprise information technology architecture. State agencies subject to 2017 SC Act No. 97, Part 1B, Section 117.121 must adhere to the standard as set forth herein.

## Agency Exception Requests

Agencies that need to deviate from the standard, and/or technologies specified in this standard, may request an exception from the Technology Work Group (TWG). In such a case, the agency must submit a written statement of their business needs to their Agency Relationship Manager in the South Carolina Department of Administration Program Management Office. The exception request must demonstrate current quantitative performance baselines, or any regulatory compliance required in their business solution. All exceptions must be approved prior to the agency pursuing procurements, deployments, or development activities related to technologies that are not compliant with this standard.

## Business Need

Hyper Converged Infrastructure Systems (HCIS) can be leveraged to meet a host of business needs currently demanded within South Carolina's enterprise information technology environments. Leading the pack is the demand for self-service capability among application development and maintenance shops, but HCIS may also be used to support various other use cases such as:

- Virtual Desktop Infrastructure (VDI)
- Server Based Computing (SBC)
- Virtual Machine Migration
- Private/Hybrid Cloud
- Remote office/Branch Office
- Relational Databases
- Dedicated Application Infrastructure

## Product Description

Hyper Converged Infrastructure Systems combine x86-based computing and storage components with intelligent software to create flexible pooled resources. The resources can be scaled up or down based

on demand into combined resource pools called "Nodes," which themselves can be combined into larger environments or pared down as needs evolve. These resources are managed through a common toolset as a single system. HCIS provides flexibility and business responsiveness beyond what traditional server/storage architectures can provide.

While HCIS can be obtained through various platforms (such as DIY solutions, software-only and hardware-based appliances), the State of South Carolina will focus the standard for HCIS around hardware-based appliances to reduce operation and support complexity that is typically associated with DIY solutions.

## Expected Benefits

It is anticipated that HCIS environments will provide the State of South Carolina with the following benefits:

- Simplified IT provisioning
- Reduced Total Cost of Ownership through reduced maintenance and operational expenses
- Improved agility and scalability of IT infrastructure through private/hybrid cloud capabilities
- Reduced IT Complexity

## Purchasing

The State of South Carolina has contracts in place with HCIS vendors. These vendors are able to meet the technical, maintenance, and training requirements of this standard, but agencies are responsible to create specifications for systems that also meet the standard prior to procurement of any system or service. Please contact your agency procurement officer for information about the existing contracts.

## Maintenance

An effective maintenance cycle is essential to ensure that devices are available and operating correctly for their specific use. HCIS solutions must be deployed and maintained to a level appropriate for the system based on:

- The classification of the data stored, processed or accessed
- The solution’s physical and technical requirements
- The manufacturer’s best practice guidelines
- Security, privacy, regulatory and statutory requirements

Each Agency that deploys an HCIS solution is required to have a formal maintenance plan for each of the items listed above.

Further, the maintenance plan must include a summary report on the following:

1. Resources needed to ensure the maintenance cycle can be administered as designed.
2. Estimated time (per week/month/year) needed to perform maintenance.

All HCIS solutions must include a maintenance contract that covers the solution for its expected life. This maintenance contract must have established SLA's that cover the solution with the following requirements.

- On-site Parts and availability should be < = to one day from distributor or support contract provider
- Four-hour response on all product support 24/7
- Software and hardware end of support life must be > = to five years
- Support for Hard Disk Drive Retention ("HDDR") services or provide on-site destruction of storage media.
- Security and operational patch and upgrades for all system component software and firmware.

Agencies may not operate HCIS without an active, in force maintenance contract with a certified HCIS vendor.

Agencies may not operate HCIS on software or firmware versions that are no longer maintained or supported by the manufacturer. The SCDIS-200 security and privacy standards require that systems have the latest stable versions of applicable security software and firmware updates.[1]

## Training

The expense and complexity of deploying, operating, and maintaining an HCIS architecture requires skilled, appropriately trained technical personnel. Investment in personnel is as important, if not more so, to the efficient, effective, and correct operation of a system than is the investment in the HCIS itself.

Therefore, each agency that deploys HCIS solutions in the enterprise must have a formal training plan. This plan can be documentation, operating guidelines, virtual or instructor led training. The form of the plan is not defined by this standard, but the plan is required. The training plan should include (but is not limited to) the following:

- Administrator Training
    - Basic and Advanced Installation
    - Reporting
    - API Integration and Customization
    - Troubleshooting and Maintenance
- Agency guidelines on the installation of software and applications

**Should an agency need help in designing a maintenance and or training plan tailored to their specific needs, they may request assistance from the Security and Architect Review Board.**

[1] See: SCDIS-200 Information and Privacy Standards v1.5 control 11.303. The NIST Special Publication 800-53 revision 4 Security and Privacy Controls for Federal Information Systems and Organizations employs similar language in its SI-2 Flaw Remediation control.

## Technical Requirements

All technical requirements for Hyper Converged Infrastructure Systems are outlined below.

1) **Hardware**
   a) Must be provided as an integrated single solution
   b) Must provide an out-of-band management facility that includes:
      i) A baseboard management controller (BMC) that is compliant with the Intelligent Platform Management Interface (IPMI) specification version 2.0, revision 1.11 or newer version
      ii) A lights-out management (LOM) technology that provides console access to the node/enclosure independent of the operating system or basic input/output system (BIOS), including remote control of keyboard, video and mouse (KVM) and the ability to mount virtual removable media.
   c) Must provide predictive failure analytics for all storage devices, random access memory (RAM) chips, power supplies, cooling fans and central processing units (CPU) and must alert the administrator of any failing components
   d) Must be able to service all power requirements even after the complete failure of one power supply
   e) Power supplies must be hot-swappable to the effect that they can be replaced without service interruption
   f) Must be able to cool the system to specifications even after the complete failure of one cooling fan
   g) Cooling fans must be hot-swappable to the effect that they can be replaced without service interruption
   h) Solid State Drives (SSD) and/or Hard Disk Drives (HDD) must be hot-swappable to the effect that they can be replaced without service interruption
   i) Must have verifiable compliance with Federal Communications Commission (FCC) Part 15, International Electrotechnical Commission (IEC) 60950-1 (or IEC 62368-1) and CE Mark
   j) Allows firmware microcode updates to be performed on any node without impacting the overall cluster service
2) **Performance and Scalability**
   a) Nodes of different hardware configurations (CPU, RAM and/or disk capacity) must be able to coexist within the same cluster or protection group. All high availability (HA) technologies must function as designed within heterogeneous clusters.
3) **Hypervisor Integration**
   a) Must have compatibility with VMware at the hypervisor layer
   b) Must provide a mechanism to place a node in a maintenance mode
      i) When a node enters maintenance mode, the system must migrate all the data it hosts elsewhere within the cluster
      ii) should integrate with the hypervisor's maintenance mode, but it is separate functionality
      iii) Placing a node in storage maintenance mode must preserve the availability and redundancy configuration of the system's data

iv) Placing a node in storage maintenance mode must not affect data availability or redundancy for longer than it takes to migrate and/or rebalance storage workloads

**4) Data Protection**

a) Must adhere to 99.999% reliability in the event a cluster suffers data loss following the total failure of one node (and therefore, the failure of all disks in that node); it must not require manually configuring affinity/anti-affinity rules in order to achieve this

b) Must support multipathing for storage subsystem input/output (I/O), including for traffic to and from any Network File System (NFS) or Internet Small Computer System Interface (iSCSI) targets presented to a hypervisor or virtual machine (VM) guest operating system (OS), as well as for replication traffic between remote sites

c) Must implement an industry-standard data integrity checking technology

d) Must protect all volatile data stores against sudden power loss, component failures and software malfunctions; this mechanism must protect against data loss during maintenance and upgrade procedures

e) Must provide the ability to replicate data to paired HCIS appliances at a remote site, subject to documented architectural guidelines and constraints, with a recovery point objective (RPO) of 20 minutes or less

f) Normal system operations must not interfere with replication operations

i) The system must not fail to replicate data because of system overhead, nor because of simultaneous migration or provisioning operations.

ii) If the HCIS provides user-definable restrictions on data replication performance, the HCIS must not exceed the maximums or fail to reach the minimums of these restrictions due to normal operations.

g) Must provide a snapshot mechanism within the storage subsystem that:

i) leverages space-efficient techniques (such as redirect-on-write or copy-on-write) for increased data efficiency and;

ii) that is independent of any write-mirroring snapshot capability inherited from the hypervisor

h) Must not require a portion of the storage capacity to be reserved, pre-allocated or dedicated to snapshots; rather, the system must dynamically allocate storage space to snapshots, on demand

i) Must adhere to 99.999% reliability in the event the system suffers data loss following the simultaneous failure of any two disks across one or multiple nodes within the same cluster or protection group.

**5) Networking**

a) Must support network links for host connectivity with a throughput of at least 10 Gbps per link.

**6) System Administration**

a) System's management graphical user interface (GUI) must be capable of managing the entire life cycle of all software-defined compute and storage including all of these functions:

(1) Creating, updating, and/or destroying VMs or containers

(2) Migrating VMs between nodes

(3) Enabling or disabling hypervisor-based capabilities on VMs

(4) Creating, updating, and/or destroying snapshots and replication targets

b) Must be able to detect error conditions in all physical and virtual infrastructure and display alerts in the management GUI; must provide a mechanism to monitor its proprietary storage subsystem, and it must provide either a means of monitoring physical hosts and VMs or a means of importing error alerts from the hypervisor
c) Must be able to assess the performance of all physical and virtual infrastructure, and display alerts in the management GUI; must provide a mechanism to monitor its proprietary storage subsystem, and it must provide either a means of monitoring physical hosts and VMs or a means of importing performance alerts from the hypervisor
d) Management GUI must provide a search function by which an administrator can rapidly locate any object or construct (such as hosts, VMs, disks and switches) by the name of the object
e) Must not require vendor self-signed certificates
f) Must have documented customer procedure to update/replace certificates
g) Must publish an application programming interface (API) that provides programmatic management of system functions

**7) Security**

a) Must have the ability to:
   i) Identify, classify, remediate, and mitigate all known vulnerabilities of its software platform from the system's management GUI
   ii) Deliver and automatically install patches for all components of its software platform from the system's management GUI
   iii) Must follow a regular patch release schedule and proactively release out-of-schedule security patches when needed
b) Must support implementing any best practices for hardening of the hypervisor that are recommended by the hypervisor vendor
c) Must permit data that is housed in VMs to be encrypted by software running in the guest-OS; this guest-OS encryption must function whether the VM uses block or object storage
d) Must encrypt all traffic on the control plane using Secure Sockets Layer (SSL) certificates that meet the latest version of the Transport Layer Security (TLS) standard
e) Must publish document security best practices for the HCIS and make them available to customers.
f) Management GUI and all APIs must support role-based access control (RBAC) security, whereby users are required to log in, and different access rights can be granted to different users
g) Must be Federal Information Processing Standard (FIPS) 140-2 Level 1-compliant (Overall System)
h) Must integrate fully with security information and event management (SIEM) tools e.g., Splunk, IBM QRadar, or VMware vRealize Log Insight
i) Secure Shell (SSH) v2 minimum for console access
j) Must encrypt all traffic to and from the management GUI using SSL certificates that meet the latest version of the TLS standard
k) Must support centralized identity services
l) Must comply with South Carolina Security Policies and Standards
m) Underlying OS must be at an actively supported version

n) Must provide the ability to create a complete backup of all system configurations and to store that backup outside the system. This must be a separate backup facility specifically for the system configuration and not something done as part of the general backup facility for applications and data.

**8) Solution EcoSystem**

a) Must have the ability to ship its logs to an external log server located in the same data center
b) Must log all events and object state changes that occur within the system
c) Must alert on System Events

**9) Service and Support**

a) Must provide a warranty of at least three years on any parts initially sold as part of the HCIS SKU, provided the part is returned to the Vendor
b) Must provide live assisted support twenty-four by seven, along with an online support knowledge base that can be accessed at any time
c) Must guarantee that, in the event the agency must return a storage device to the Vendor, the data on it will be handled confidentially and securely. If the device will not be returned to the agency, the Vendor will destroy all agency data residing on the device, or destroy the device itself, according to the agency's specifications and provide a certified record of destruction.
d) Must offer support options that are guaranteed to address problems by the next business day following the agency's report, or sooner. This support must be available at all agency locations
e) Must have a testing and certification process for peripherals and publish hardware compatibility lists for peripherals certified to work with the system
f) Must publish reference architectures for configuring popular enterprise applications or use cases on the HCIS
g) Must include a "call home" facility that can notify the Vendor of error conditions without human intervention which can be disabled

## Technology Adoption

This section lays out the technology roadmap vis-à-vis Hyper Converge for the state while recognizing that not all agencies are currently at the same place technologically. When procuring and/or implementing new or upgraded HCIS systems, agencies must adopt either the Emerging or Strategic Technology Tier. If an Agency find themselves in the Contained or Obsolete Technology categories, they must begin planning now to adopt the Strategic Tier no later than when their next technology refresh is scheduled to take place.

### Emerging Technologies

HCIS technology is Emerging in nature to the state and therefore the standard as written is the Emerging Technology standard. Agencies may adopt the Emerging standard as appropriate to their needs.

### Strategic Technologies

Non-applicable.

## Contained Technologies

Non-applicable.

## Obsolescent/Rejected Technologies

Non-applicable.

# Appendix A

## Optional Technical Capabilities for Hyper Converged Infrastructure Systems

### Hardware

- Supports out-of-band management that conforms to the latest version of the Redfish standard published by the Distributed Management Task Force
- Supports booting to a Pre-boot Execution Environment (PXE) for bare-metal Operating System (OS) deployment
- Includes a dedicated secure crypto processor that complies with Trusted Platform Module (TPM) main specification
- Supports multiple flash types
- Supports maximum memory configuration for each node at least 512GB RAM or greater
- Supports cooling fans that automatically adjust speed and/or direction to keep components cooled to within specification while consuming the least possible amount of electricity
- Supports a minimum of one general-purpose graphics processing unit (GPGPU) per node of any make and model that is supported by both the hardware manufacturer and the installed OS
- Supports multilevel cell (or denser) Solid State Device (Drive) (SSDs)
- Supports fourth-generation double data rate (DDR4)
- Supports Dynamic Random-Access Memory (DRAM) Double Device Data Correction (DDDC)
- Allows ability to rekey locks on Vendor provided equipment racks
- Supports single-phase consumer power sources

### Performance and Scalability

- Enterprise scalability (at least 64 nodes)
- Supports two-node clusters
- Offers storage-heavy nodes, meaning at least four hard-disk bays that can be clustered with standard two-disk bay models and that allow for greater storage capacity per node
- Offers some means to add only storage capacity to the cluster without simultaneously adding to its compute capacity
- Bypasses hypervisor Input / Output (I/O) latency
- Provides predictive capacity analytics for all storage devices, RAM chips, power supplies, cooling fans and CPUs

### Hypervisor Integration

- Supports latest major release of VMware vSphere
- Supports latest major release of Hyper-V Server
- Supports latest major release of Xen
- Supports latest major release of Acropolis
- Supports running compute workloads in containers

## Data Protection

- Utilizes some form of erasure coding for at least a subset of its data
- Provides global storage namespace(s) for metro-area clusters that span multiple physical locations
- Availability greater than or equal to 99.9999% (six 9s); these uptime claims are rationalized with independent testing, reference customers or field data
- Administrators can choose an Redundancy Factor (RF) on a per-VM or per-vDisk basis
- Provides the option to disable High Availability (HA)/data protection on a per-VM or per-vDisk basis
- Provides the ability to keep the replication of a grouped set of volumes or data artifacts consistent
- Provides the ability to replicate data to paired HCIS appliances located at a remote site with recovery point objective (RPO) times approaching zero
- Offers fully synchronous replication to paired HCIS appliances located at a remote site
- Has the capability to build node clusters that span multiple physical locations, and it utilizes all cluster nodes simultaneously in an active-active model
- Supports the creation of rapidly provisioned, space efficient read-only and read/write clones of all data volumes or artifacts independent of any cloning functionality inherited from the hypervisor
- Can schedule periodic snapshots of VMs and/or virtual disks
- Provides direct recovery of virtual disks in a single step
- Capable of leveraging the Microsoft Windows Volume Shadow Copy Service (VSS) to create application consistent snapshots for Windows VMs
- Supports creating a virtual disk that is larger than the available storage capacity of the node on which it resides
- It is impossible to suffer permanent data loss following the total failure of two nodes simultaneously
- It is impossible to suffer data loss following the simultaneous failure of any three disks in the same cluster or protection group
- Ransomware protection strategy
- Provides user-definable retention policies for snapshots that are enforced automatically

## Data Services

- Reserves a portion of the system RAM to be used as a cache for I/O streams
- Makes SSDs available as a primary storage medium (that is, used for storing data rather than just for file metadata or caching), and it automatically migrates in-demand blocks of data from slower disk types
- Deduplicates data that is housed in the performance tier
- Deduplicates data that is housed in the capacity tier
- Performs data deduplication in-line rather than postprocess
- Deduplicates data across all storage media in all hosts visible to the system, without regard to protection groups or clusters
- Compresses data that is housed in the performance tier
- Compresses data that is housed in the capacity tier

- Performs data compression in-line, rather than postprocess
- Compresses data across all storage media in all hosts visible to the system, without regard to protection groups or clusters
- Ability to deduplicate and compress the same block of data at the same time. If the system can deduplicate OR compress a block of data, but not both simultaneously on the same block, this does not satisfy this criterion
- Ability to enable and disable the data services it provides on a per-vDisk basis
- Ability to guarantee each virtual disk a minimum amount of available bandwidth and to limit the bandwidth being used by any one virtual disk, as specified by the user
- Stores file and/or disk metadata on the fastest available storage medium to optimize I/O performance
- Ability to enable and disable the data services it provides on a per-VM basis
- Ability to guarantee each VM a minimum amount of available bandwidth and to limit the bandwidth being used by any one VM, as specified by the user
- Cache writes to an SSD to optimize I/O performance

## Networking

- All I/O interfaces support both the Intel single-root I/O virtualization (SR-IOV) and multi-root I/O virtualization (MR-IOV) standards
- Network interfaces include a hardware TCP/IP offload engine
- All system I/O interfaces support NFB using the VMware VXLAN protocol
- Supports remote direct memory access (RDMA) for its network links
- Supports network links with speeds of 1 Gbps per link for host connectivity
- Includes a physical Ethernet switching facility capable of routing Layer 2 traffic and of serving as a VXLAN Tunnel Endpoint (VTEP) termination endpoint
- Supports micro-segmentation for increased security and better policy-driven network management
- Supports network function virtualization (NFV)
- Supports more than 10Gb throughput per port
- Built in integration with a Software Defined Networking (SDN) product and capable of managing SDN functions directly from its management GUI

## System Administration

- Management GUI is capable of managing the entire life cycle of on-premises infrastructure, including all of these functions:
    1. Configuration of BIOS/Unified Extensible Firmware Interface (UEFI) settings on newly deployed nodes;
    2. automatic installation of the hypervisor or container OS on a node;
    3. building host clusters and resource pools at the hypervisor level;
    4. creating, updating, and/or destroying hypervisor data stores;
    5. creating or destroying vSwitches at the hypervisor level, and connecting/disconnecting hypervisor hosts from these vSwitches; and
    6. if the system includes physical switches, then provisioning and management of all physical switch functions

- Ability to provision public cloud IaaS instances to Amazon Web Services (AWS) and to manage the full life cycle of a deployed instance, either by leveraging the AWS APIs directly or by deploying the HCIS software to AWS
- Ability to provision public cloud IaaS instances to Microsoft Azure and to manage the full life cycle of a deployed instance, either by leveraging the Azure APIs directly or by deploying the HCIS software to Azure
- Detects when an object it manages changes configuration such that it no longer matches its originally configured desired state, then triggers an alter in the management GUI
- Management GUI is a web-based console that functions on any OS, using any browser that is capable of executing the latest version of HTML and Cascading Style Sheets (CSS); it must not require the installation of additional software (including agents or browser plug-ins) to use the GUI and should be responsive to and optimized for mobile device browsers
- Management GUI allows users to create and customize dashboards, displaying information that they choose about any object managed in the GUI
- Management GUI provides recommendations that guide the administrator in configuring VMs, virtual disks, and hosts for optimal capacity utilization
- Management GUI provides recommendations that guide the administrator in configuring VMs, virtual disks and hosts for optimal performance
- Ability to monitor system capacity over time and then to provide detailed projections of future system utilization and the time to resource exhaustion on the current trend
- Has mechanism to enforce policies set by the administrator on all objects it manages and to correct any configurations that do not match the specified policy automatically
- Management GUI has ability to assess which system alerts are most critical and to alert the administrator only for alerts that exceed a severity threshold specified by the administrator
- Ability to migrate existing VMs running on on-premises hosts to all public cloud IaaS providers that it supports
- Publishes an SDK that provides native programmatic management of system functions in one or more programming languages
- Management GUI provides a search function by which administrator can rapidly locate any object or construct (such as hosts, VMs, disks and switches) by the most common properties or characteristics of that object (such as IP address, folder, label, or the value of custom free text fields)
- Update to HCIS that does not interrupt access to data or system service
- Provides a tool that can generate a map of all infrastructure components that comprise the HCIS, as well as the relationships between them

## Security

- Implements or integrates with a network intrusion prevention system (NIPS)
- Complies with Payment Card Industry Data Security Standard (PCI DSS)
- Complies with IRS Pub 1075 (Tax Information Security Guidelines for Federal, State and Local Agencies) / Safeguard Computer Security Evaluation Matrix (SCSEM)
- Complies with Defense Information Systems Agency (DISA) Security Technical Information Guide (STIG) security standard
- Complies with Health Insurance Portability and Accountability Act (HIPAA)
- Complies with Criminal Justice Information Systems (CJIS) Security Requirement

- Implements two-factor authentication (2FA) for logins to the management GUI
- Integrates fully with network forensics tools (NFTs) e.g., Blue Coat, FireEye
- Supports full-disk encryption (FDE)
- Supports self-encrypting drives (SEDs)
- Customer access to system root
- Vendor has access to the entire control plane source code and can implement changes, either because the code is proprietary to the vendor or because it is open source
- Management GUI integrates fully with one or more identity providers, such as Microsoft Active Directory Federation Services (ADFS) or HyTrust
- Controller based data encryption

## Solution EcoSystem

- Integrates fully with at least one cloud management platform (CMP) by providing connectors, interfaces, or APIs that are necessary for the CMP to manage all components of the HCIS - or the system includes a proprietary CMP of equal capabilities
- Supports IPv6 for all components
- Ability to export capacity in its software-defined storage pool for use by other servers in the same data center using one of the following file-based storage protocols: Common Internet File System (CIFS), Server Message Block or NFS
- Ability to export capacity in its software-defined storage pool for use by other servers in the same data center using a block-based storage protocol such as iSCSI
- Ability to import any data store presented to and configured within the hypervisor and to add that capacity to its software-defined storage pool
- Ability to import external file-based storage presented to it via the NFS, Server Message Block or CIFS protocols and to add that capacity to its software-defined storage pool +
- Ability to import external block-based storage presented to it from a supported array and to add that capacity to its software-defined storage pool
- Integrated with OpenStack in such a way that it can host all the following OpenStack services: Nova (compute), Cinder (block storage) and Neutron (networking)

## Service and Support

- Vendor provides a single point of contact for any support or service request for any product sold as part of the HCIS SKU including the hardware, firmware, hypervisor and HCIS software layer
- Vendor has a dedicated service account manager (SAM) as a support option; the SAM need not be deployed to the agency's site
- Customer Replaceable Drives
- Vendor provided instructor-led training
- Vendor provides a resident engineer as a paid support option. The resident engineer should be on-site at the customer's specified work location for a minimum of 20 hours per normal workweek, unless the agency specifies fewer hours
- Vendor provides a warranty of at least five years on any defective part sold as part of the HCIS SKU, provided the part is returned to the vendor
- Vendor offers support agreements for third-party products whether those are sold as part of the HCIS SKU

- Vendor offers 24/7 live support as an option
- Vendor offers support options that are guaranteed to address problems on the same business day that they are reported
- Vendor does not charge for upgrades to its software platform, including its management GUI, for the duration of the customer's support contract. This must apply even when new software versions add previously unavailable features.
- Vendor offers the option to dispatch its own personnel to the agency's site to qualify and tune the performance of the agency's HCIS
- Vendor provides a written guarantee of the HCIS's availability, performance or storage efficiency. The guarantee must specify any limitations regarding configurations, workloads or feature usage.
- Vendor offers assistance in determining the root cause of any problem that arises with the HCIS and it prepares a formal root cause analysis report at the agency's request
- Vendor offers the option to utilize United States Based Support in which no part of the resulting services is performed offshore of the United States, by persons located offshore of the United States, or by means, methods or communications that, in whole or in part, take place offshore of the United States
- The vendor supplies spare parts that are to be kept by the agency on-site and replaced by the customer as needed at no extra charge
- Support provisions are available for the agency to retain physical storage drives for agency destruction
- Vendor agrees to sign any business associate agreements (BAAs) the agency may require to stay in compliance with regulations