

1.5.2 Collocated Hosting Services (CHS) [C.2.4.3]

Agencies will fulfill e-Gov mandates and Federal Enterprise Architecture (FEA) initiatives by collocating equipment and implementing critical applications within a fully compliant Collocated Hosting Services (CHS) provider data center. A reliable, secure, scalable, and globally available CHS will be supplied through a full service provider offering a high-availability Internet protocol (IP) backbone network, an extensive hosting service portfolio and outstanding web-based monitoring and management.

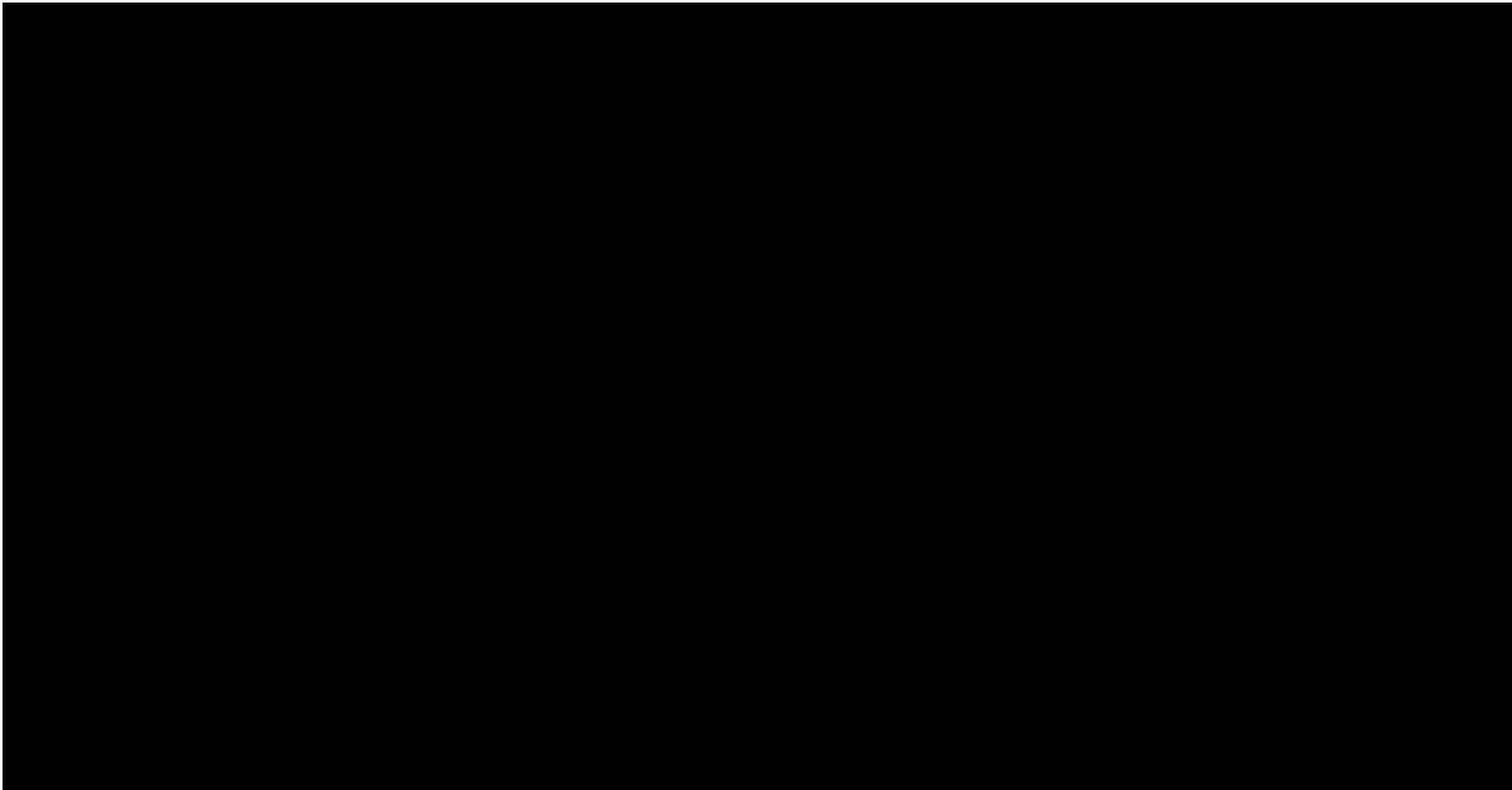
1.5.2.1 Technical Approach to Management and Applications Service Delivery [L.34.1.5.1]

1.5.2.1.a Approach to Service Delivery

(a) Analyze the service requirements specified in this solicitation and describe the approaches to service delivery for each service.

AT&T's Enterprise Hosting Services is a continuum of hosting and management capabilities providing Agencies a global, scalable, reliable, and flexible infrastructure to run e-business applications. As a component of Enterprise Hosting Services, CHS allows Agencies to collocate equipment within an AT&T Internet Data Center (IDC). CHS provides an array of hosting services designed to allow Agencies to implement enterprise class e-business applications that address their needs and challenges.

AT&T's CHS enables Government Agencies to locate their own equipment in an AT&T IDC. From this secure conditioned environment, Agencies can connect directly to the AT&T Internet protocol (IP) backbone. **Figure 1.5.2.1-1** shows the CHS architecture with many of the service elements available to Agencies to collocate their equipment in a CHS environment.



Agencies can take advantage of the available service elements to create a high-availability, secure CHS.

AT&T will provide the Government with a highly available, flexible, and secure CHS that will exceed the Government’s requirements. **Table 1.5.2.1-1** discusses the approach to service delivery of a CHS solution.

APPROACH	DESCRIPTION
Operate IDC under defined Physical and Security Standards	<div style="display: flex;"> <div style="writing-mode: vertical-rl; transform: rotate(180deg); font-weight: bold; margin-right: 5px;">N+1 Redundancy</div> <div> <p><i>IDC Power</i>-Uninterruptible power supply (UPS), backup diesel generators</p> <p><i>IDC Physical Security</i>-Physical security guard, mantrap doors, electronic badge, and biometric readers</p> <p><i>IDC Logical Security</i>-Firewall and intrusion detection services (IDS)</p> <p><i>IDC Air Conditioning</i>-Computer room air conditioning (CRAC) systems</p> <p><i>IDC Smoke Detection and Fire Suppression</i>-Dry pipe system and very early smoke detection apparatus (VESDA) system</p> </div> </div>
Provide Facilities-Based IDCs and interconnect to leading Tier 1 Internet Service Provider (ISP)	<ul style="list-style-type: none"> • AT&T owns, operates, and manages all IDCs and facilities • AT&T operates the largest Tier 1 ISP, transmitting 2.5 petabytes of traffic through the network daily (equivalent to 120 times the text volume of the Library of Congress) • Extensive private peering arrangements with other ISPs • High availability ISPs
Provide Host Administrative Tasks (Remote Hands)	Remote Hands is provided to client-managed Agencies, if requested, and for an additional fee, and it involves basic activities of an onsite AT&T technician acting as the <i>eyes, ears, and fingers</i> on the Agency’s behalf.
Provide Client Networking Options	<p>AT&T offers the following optional services for Agencies subscribed to CHS:</p> <ul style="list-style-type: none"> • AT&T Managed Local Area Network (LAN) Switching • AT&T Out-of-Band Management Hardware (HW) • Managed Local Load Balancing (LLB) • Managed Local Load Balancing – High Availability (LLB-HA) • Managed Global Balancing (GLB)

Table 1.5.2.1-1: Approach to CHS Delivery. Agencies can subscribe to a CHS that will be delivered with high availability and security.

CHS will provide Agencies with a high availability and secure hosting environment, along with client networking options to best suit an Agency’s specific hosting and networking requirements.

1.5.2.1.b Benefits to Technical Approach

(b) Describe the expected benefits of the offeror’s technical approach, to include how the services offered will facilitate Federal Enterprise Architecture objectives (see <http://www.whitehouse.gov/omb/egov/a-1-fea.html>).

AT&T’s Networx services, in general, and CHS, in particular, support the Government’s vision of transformation through the use of the Federal Enterprise Architecture (FEA) by providing the technologies that contribute to the Agency’s mission objectives. **Table 1.5.2.1-2** describes each service in relation to FEA, summarizes its contribution, and/or provides an example of how it facilitates FEA implementation.

SERVICE DELIVERY APPROACH	BENEFITS	FEA FACILITATION
Operate IDC under defined Physical and Security Standards	Agencies benefit from AT&T's high standards of IDC infrastructure elements by attaining a high level of redundancy and reliability within the IDC and a safe, secure environment for their applications hosted on CHS facilities.	As a component of Technical Reference Model (TRM)/service platform and infrastructure/hardware/infrastructure, Agencies can feel comfortable that their web, media, and application servers are securely located in a reliable, disaster tolerant hosting environment.
Provide Facilities-Based IDCs and interconnect to leading Tier 1 ISP	AT&T owns and operates all of its hosting facilities, as well as owning, operating, and managing its global IP network, which greatly helps Agencies receive end-to-end superior performance from application to Agency end user.	As a component of TRM/service platform and infrastructure/hardware/infrastructure, Agency applications and services will be securely placed in IDCs that are fully managed and monitored by AT&T and not by a third party contracting to AT&T.
Provide Host Administrative Tasks (Remote Hands)	Agencies without enough manpower can benefit with onsite AT&T technician to perform tasks on their equipment.	As a component of TRM/service access and delivery/service requirements, Agency equipment is easily accessed by authorized, onsite technicians to assist remote Agency personnel with equipment issues.
Provide Client Networking Options	Agencies will know that they can reach their hosting equipment remotely, and that their hosting equipment has high availability to their end users and constituents.	As a component of TRM/service access and delivery/service transport, Agency applications are accessed by Agency personnel, end users and constituents through several methods of service transport and out-of-band access.

Table 1.5.2.1-2: Agency Benefits and FEA Facilitation. Agencies can receive products and services components that are easily integrated, commonly manageable, and aligned to support FEA objectives and meet FEA guidelines.

AT&T's development of net-centric technologies supports solutions based on service oriented architecture (SOA), which uses standardized, web-adapted components. Our approach ensures that the criteria listed below are followed:

- TRM capabilities are fully met and linked to the Service Component Reference Model (SRM) and Data Reference Model (DRM).
- These links are structured to support Business Reference Model (BRM) functions and provide line-of-sight linkage to mission performance and ultimate accomplishment per the Performance Reference Model (PRM)
- AT&T operates as an innovative partner through Networx to help achieve the vision of the FEA to enhance mission performance.

In addition to the benefits and FEA facilitations cited earlier, AT&T will assist specific departments and Agencies to meet mission and business objectives through a comprehensive CHS offering.

1.5.2.1.c Major Issue to Service Delivery

(c) Describe the problems that could be encountered in meeting individual service requirements, and propose solutions to any foreseen problems.

In transitioning into any new service delivery model, whether it be task-based or fully outsourced, unforeseen issues can always arise. Therefore, it is important that GSA selects a service provider, such as AT&T, which brings the depth and background that minimize an Agency’s risk during transition. Our experience has enabled us to develop proven methods, processes, and procedures applicable to the simplest or the most complex projects.

Table 1.5.2.1-3 lists the top seven service delivery risks and our mitigation strategy. [REDACTED]

[REDACTED]

RISKS	RISK DESCRIPTION	RISK MITIGATION
Business Disruption	In our experience, all Agencies are concerned about business disruption, particularly when applications are not available for use.	[REDACTED]
Requirements Changes	Requirements changes before and after service delivery contribute to budget overruns, schedule slips, and missed expectations.	[REDACTED]

RISKS	RISK DESCRIPTION	RISK MITIGATION
Lack of Implementation Support	In certain implementations, requirements can go undefined, staffing could be inadequate, and delivery dates might be missed.	[REDACTED]
Equipment Functionality	It is not uncommon for service enabling devices (SEDs) to not live up to manufacturer's claims and fail to deliver the functionality that the customer expects.	[REDACTED]
Role Confusion	Custom-managed service projects can experience role confusion between organizations	[REDACTED]
Security Threats	Security threats are a great risk in moving to a new data center or an outsourced managed environment.	[REDACTED]
Network Facilities	Network facilities not available to be deployed when the Agency requests the service.	[REDACTED]

Table 1.5.2.1-3: AT&T Service Delivery Lessons Learned and Risk Mitigation Strategies. Agencies benefit from lessons learned and experience implementing CHS, which ultimately minimizes service delivery risks.

AT&T has taken steps to identify risk and provide risk mitigation associated with delivering CHS. AT&T is committed to service excellence and will work with the Agency to identify and resolve potential problems that might occur during service delivery.

1.5.2.2 Satisfaction of Management and Applications Performance Requirements [L.34.1.5.2]

1.5.2.2.a Service Quality and Performance

(a) Describe the quality of the services with respect to the performance metrics specified in Section C.2 Technical Requirements for each service.

Agencies will access a high quality network that sets the industry quality standards for performance. AT&T will meet the performance levels and

acceptable quality level (AQL) of key performance indicators (KPIs) for CHS, as presented in the RFP and **Table 1.5.2.2-1**.

KEY PERFORMANCE INDICATOR (KPI)	USER TYPE	PERFORMANCE STANDARD (LEVEL/THRESHOLD)	PROPOSED SERVICE QUALITY LEVEL
Availability (Internet Connection)	Routine	99.99%	[REDACTED]
Availability (Site Power)	Routine	100%	
Time to Restore (TTR)	Without dispatch	4 hr	
	With dispatch	8 hr	

Table 1.5.2.2-1: CHS Performance Parameters. Access to Agency hosted infrastructure is maximized through a high-quality CHS supported and that complies with CHS key performance indicators listed above.

By meeting the AQLs for the specified KPIs, AT&T will provide Agencies with a high-availability network and CHS.

1.5.2.2.b Approach to Monitoring and Measuring Performance

(b) Describe the approach for monitoring and measuring the Key Performance Indicators (KPIs) and Acceptable Quality Levels (AQLs) that will ensure the services delivered are meeting the performance requirements.

For each KPI associated with CHS, AT&T has a methodology for measuring and monitoring each KPI. **Table 1.5.2.2-2** describes the approach for monitoring and measuring the KPIs, as listed in this section by the Government.

KEY PERFORMANCE INDICATOR (KPI)	APPROACH TO MONITORING AND MEASURING
Internet Availability	[REDACTED]
Availability (Site Power)	[REDACTED]

KEY PERFORMANCE INDICATOR (KPI)	APPROACH TO MONITORING AND MEASURING
Time to Restore (TTR)	[Redacted]

Table 1.5.2.2-2: Monitoring and Measuring Performance. Agencies are provided with performance metrics that comply with Government KPIs, based on the measurement methodologies.

Agencies will benefit from AT&T’s approach to monitoring and measuring the CHS KPIs by having comprehensive methods and procedures for monitoring and measuring KPI.

1.5.2.2.c Approach to Perform Service Delivery Verification

(c) Describe the offeror’s approach to perform verification of individual services delivered under the contract, in particular the testing procedures to verify acceptable performance and Key Performance Indicator (KPI)/Acceptable Quality Level (AQL) compliance.

Along with monitoring and measuring KPIs, there must also be a way to test and verify that AT&T is able to meet, if not exceed, the stated KPIs.

Table 1.5.2.2-3 describes verification and testing procedures for the KPIs listed by the Government. These measures will be conducted as a service average at turn-up verification as proof of performance.

KEY PERFORMANCE INDICATOR	VERIFICATION APPROACH	TESTING PROCEDURES
Availability (Internet Connection)	[Redacted]	[Redacted]
Availability (Site Power)	[Redacted]	[Redacted]

KEY PERFORMANCE INDICATOR	VERIFICATION APPROACH	TESTING PROCEDURES
		[REDACTED]
Time to Restore (TTR)	[REDACTED]	[REDACTED]

Table 1.5.2.2-3: Service Delivery Verification. The KPIs are closely monitored through a comprehensive verification approach and testing procedure that certifies the service performance [REDACTED]

AT&T takes the extended measures to test and verify network and hosting performance data, comparing the data against the stated KPIs to confirm the stated AQLs are being met, if not exceeded.

To simplify the verification process, AT&T has automated the process. [REDACTED]

[REDACTED] The service verification process is presented in greater detail in Section 1.3.2.d, Approach to Perform Service Delivery Verification.

1.5.2.2.d Performance Level Improvements

(d) If the offeror proposes to exceed the Acceptable Quality Levels (AQLs) in the Key Performance Indicators (KPIs) required by the RFP, describe the performance improvements.

The performance characteristics of AT&T’s hosting facilities, combined with high-capacity network connectivity, [REDACTED]

[REDACTED] **Table 1.5.2.2-4** lists the key AT&T core performance improvements, as compared to the RFP performance targets, along with some typical measurements taken over a three-month period.

KPI	NETWORX AQL THRESHOLD	AT&T PROPOSED AQL THRESHOLD	IMPROVEMENT PERCENTAGE
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]

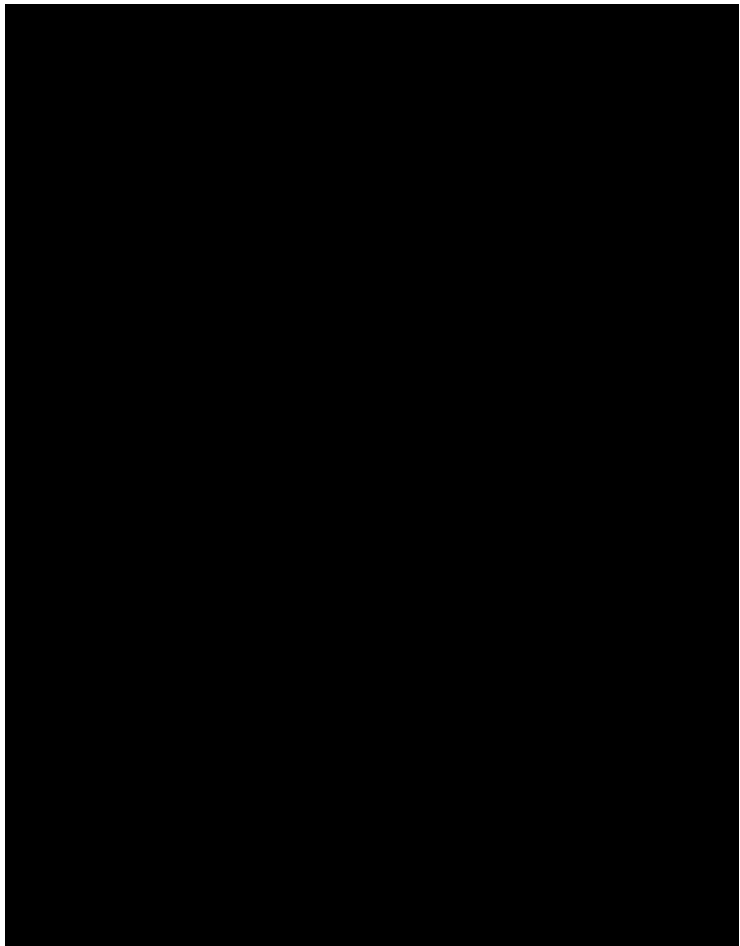
KPI	NETWORK AQL THRESHOLD	AT&T PROPOSED AQL THRESHOLD	IMPROVEMENT PERCENTAGE
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]

Table 1.5.2.2-4: Performance Level Improvements. [REDACTED]

1.5.2.2.e Approach and Benefits for Additional Performance Metrics

(e) Describe the benefits of, and measurement approach for any additional performance metrics proposed.

The KPIs defined by the Government for CHS will provide a comprehensive assessment for service verification and service performance monitoring. Therefore, AT&T does not propose additional KPIs for CHS.



1.5.2.3 Satisfaction of Management and

Applications Service Specifications [L.34.1.5.3]

1.5.2.3.a Service Requirements Description

(a) Provide a technical description of how the service requirements (e.g., capabilities, features, interfaces) are satisfied.

AT&T's CHS offering consists of a number of components starting with the equipment architecture of an IDC (**Figure 1.5.2.3-1**). **Table 1.5.2.3-1**

Figure 1.5.2.3-1: IDC Architecture. [REDACTED]

provides a narrative of the equipment architecture and other components of the CHS offering.

SERVICE REQUIREMENTS	DESCRIPTION	BENEFITS TO AGENCY
IDC Architecture	[REDACTED]	Agencies will have maximum uptime in an AT&T hosting environment based N+1 redundancy of IDC hardware and connectivity.
Analog Line	Analog telephone line is available to Agencies for out-of-band management of collocated equipment.	Agencies have 24x7 remote access to their collocated equipment for configuration or trouble management.
Cabinets/Cages: Rack Options	Quarter-, half-, and full-rack options are available to Agencies.	Agencies can subscribe to a specific amount cage space, as required.
Cabinets/Cages: Lockable Cabinet	<ul style="list-style-type: none"> • Cabinets are four-post racks with lockable doors and side panels and can be used inside or outside a cage. • Dimensions are 24 in. wide (outside) x 36 to 39 in. deep and 42 to 45 U tall, depending on IDC. Inside width is 19 in. • If the cabinet is outside a cage, there could be sides on the cabinet or between cabinets. • If inside the cage, there will be end panels on the end cabinets. 	Agencies can feel secure that their collocated equipment is safe from unauthorized physical access.
[REDACTED] (Host Administrative Tasks)	<p>Agencies, managing their own hosting service, can order Remote Hands services if they determine they require onsite IDC support from an onsite AT&T technician, serving as the <i>eyes, ears, and fingers</i> of the Agencies. The components of Remote Hands are listed below:</p> <p>[REDACTED]</p>	Agencies can save on manpower and travel to IDCs by “employing” an onsite AT&T technician to perform certain tasks on Agency equipment and within Agency cage space.
Basic Monitoring Service	Includes ping and port monitoring services	Agencies will know the up/down status of their collocated equipment.
Web Reporting	<p>The AT&T managed services portal is an online gateway to real-time information about a customer’s AT&T-hosted infrastructure. Portal users receive customized, secure access to information about their managed hosting service, including:</p> <p>[REDACTED]</p>	Agencies can view their managed hosted environment metrics through a web portal at anytime.
Seismic Bracing	AT&T’s IDCs in Seismic Zone Numbers 3 and 4 are constructed to comply with local earthquake zoning codes.	Agency collocated equipment is protected from the physical effects of earthquakes.

SERVICE REQUIREMENTS	DESCRIPTION	BENEFITS TO AGENCY
Storage Media Change	[REDACTED]	Agencies can save on manpower and travel to IDCs by allowing onsite technicians to change Agency storage media.
Network Connectivity: Internet Front End Connectivity	Provides Internet access to AT&T IP backbone on an Ethernet handoff from IDC infrastructure. [REDACTED] Front-end connectivity interfaces and speeds are as follows: <ul style="list-style-type: none"> • 10 Mbps Ethernet • 100 Mbps Fast Ethernet • 1 Gbps Gig Ethernet 	Agencies will have high-speed connectivity to the Internet for their managed hosted environment.
Network Connectivity: Back-End Connectivity	At a minimum, back-end connectivity provides cross-connect cabling between one cage demarcation, such as a carrier cage, and another cage or cabinet. Back-end connectivity can include additional services (options): <ul style="list-style-type: none"> • Shared Frame Relay • 64 or 128 kbps • Total Service Plain Old Telephone Service (POTS) • Copper cross-connect cabling • Coax cross-connect cabling • Fiber cross-connect cabling 	Agencies can cross-connect their collocated equipment to other services, allowing Agency personnel, end users and constituents to access applications from other AT&T services, such as the frame relay network.
Network Connectivity: Shared Multi-ISP	AT&T will provide the following services: [REDACTED]	Agency end users and constituents are provided maximum uptime of access to their applications through an auto-failover design of the Internet connectivity, as well as a single POC for all of their managed Internet connectivity needs within the IDC, from the router, to the access, to the multiple ISP backbones
Network Connectivity: Dedicated Multi-ISP with Local Loop	AT&T will provide the following services: [REDACTED]	
Network Connectivity: Dedicated Multi-ISP without Local Loop	AT&T will provide the following services: [REDACTED]	
CHS/Global Internet Data Center (GIDC) Environment	GIDC architecture consists of over [REDACTED] in North/South America and Continental Europe. GIDC environment consists of three elements: <ul style="list-style-type: none"> • Commercial and backup power • Air conditioning and ventilation • Smoke detection and fire suppression Each element will be discussed in further details in this subsection.	Agencies benefit by attaining a high level of redundancy and reliability within the IDC, and a safe and secure environment for their applications hosted on CHS facilities.

Table 1.5.2.3-1: Service Description. Agencies will be able to use the technical components to develop a CHS offering suited to their requirements.

1.5.2.3.a.1 Hosting Network

As shown in **Figure 1.5.2.3-2**, all IDCs are located either with an Internet gateway node or a backbone node, providing for high-speed access from the CHS directly to AT&T's IPS backbone or another ISP through a gateway node.

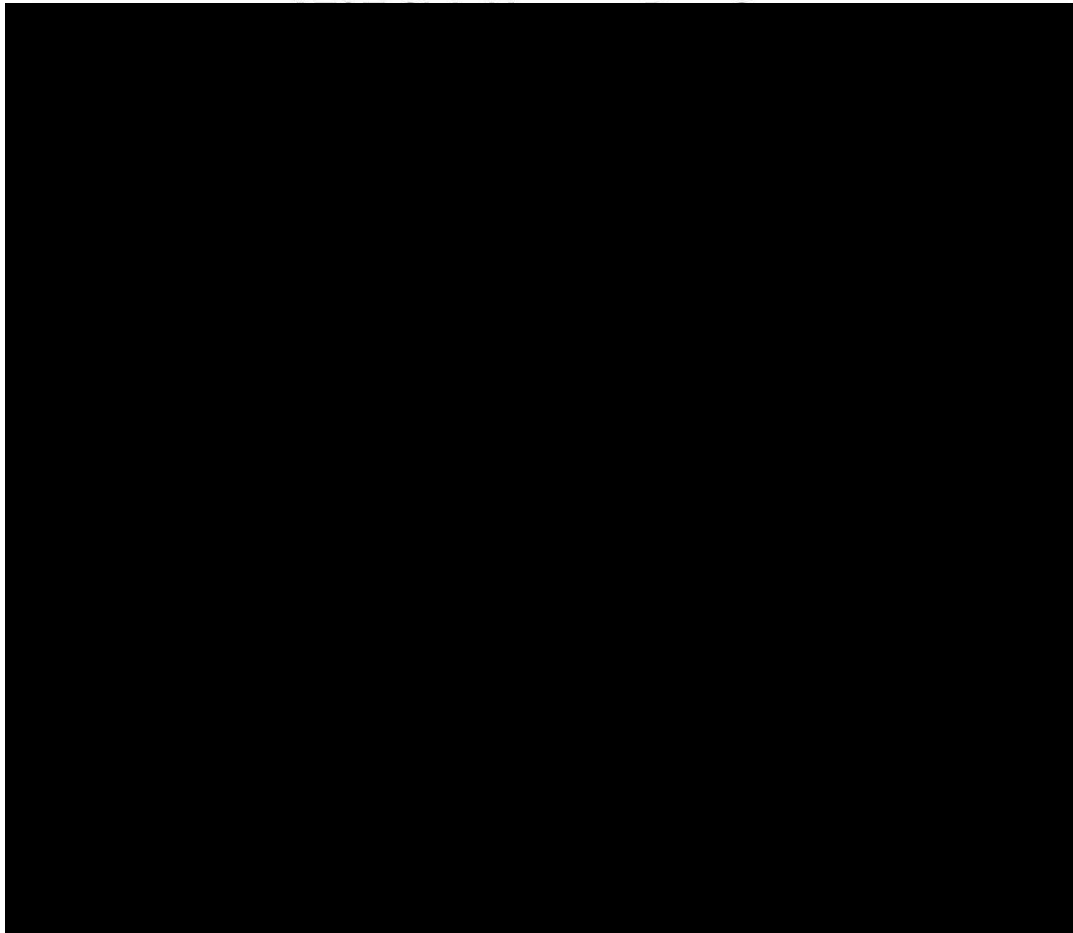


Figure 1.5.2.3-2: AT&T Hosting Network Infrastructure.

Inclusive of the IDCs (**Figure 1.5.2.3-2**), CHS facilities span worldwide, as listed in **Table 1.5.2.3-2**.

GLOBAL CHS FACILITIES			
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]

GLOBAL CHS FACILITIES			
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]

Table 1.5.2.3-2: Worldwide CHS Facilities. AT&T CHS facilities have worldwide coverage.

AT&T's worldwide CHS facility coverage provides Agencies with the benefit of deploying servers and applications to reach users globally. [REDACTED]

[REDACTED]

1.5.2.3.a.2 Power Architecture

Figure 1.5.2.3-3 displays the aspects of commercial and backup power and power conditioning in a GIDC, followed by Table 1.5.2.3-3, which discusses the GIDC power architecture in further detail.

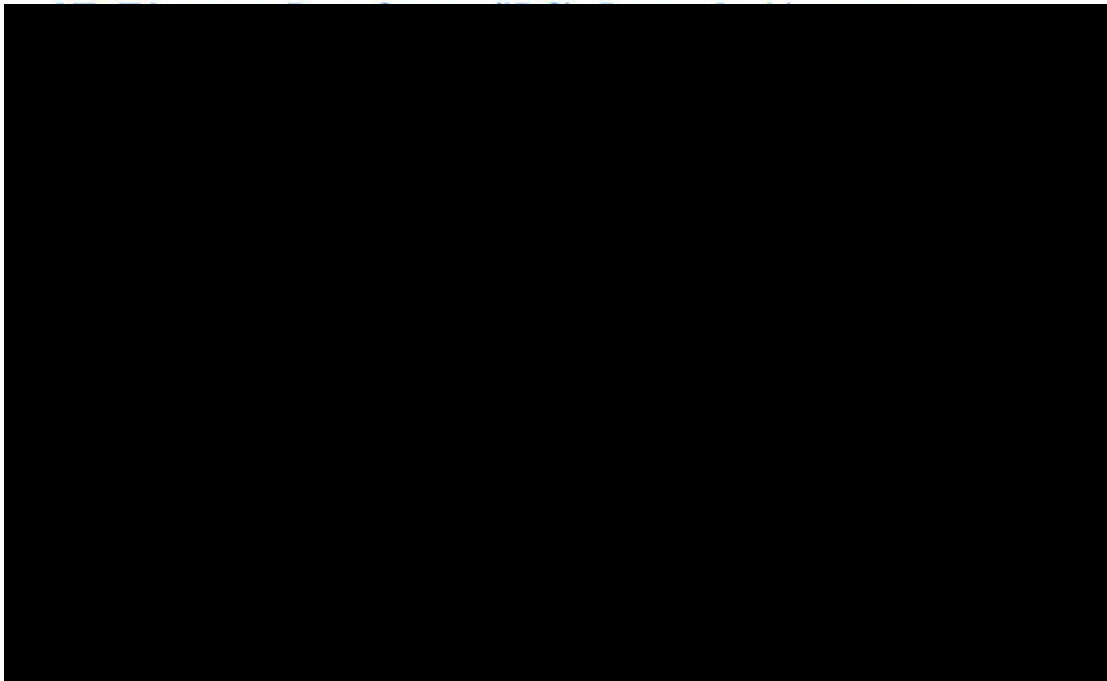


Figure 1.5.2.3-3: GIDC Power Architecture. [REDACTED]

COMPONENT	DESCRIPTION
CHS/GIDC power architecture	All GIDCs are facilities-based. AT&T owns the entire physical infrastructure. Inclusive of the physical environment are the following devices: [REDACTED] Power Handling. [REDACTED]

COMPONENT	DESCRIPTION
	<ul style="list-style-type: none"> • Diesel Power Generation: [REDACTED] • Onsite Fuel Reserves: [REDACTED] • Conditioned Power: [REDACTED] • Power Distribution Units (PDU): [REDACTED] • Remote Power Panels (RPPs): [REDACTED] • Grounding Architecture: [REDACTED]

Table 1.5.2.3-3: GIDC Power Architecture. [REDACTED]

The redundant power architecture, within an IDC, is designed for no interruption to the hosting infrastructure in the case of a commercial power failure. Therefore, end users and constituents will experience no impact to their ability to reach certain Agency application or website in the event of a commercial power failure.

1.5.2.3.a.3 Computer Room Air Conditioning

Proper ventilation and cooling is vital to the stability of CHS servers. **Figure 1.5.2.3-4** displays the different elements that are part of a GIDC air conditioning system. **Table 1.5.2.3-4** discusses the details of air conditioning for a GIDC.

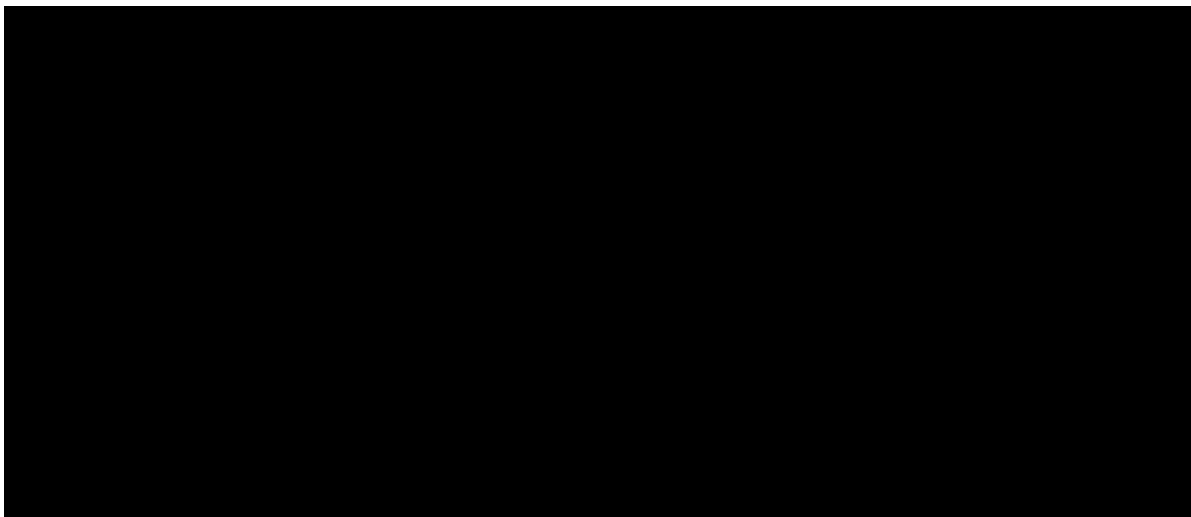


Figure 1.5.2.3-4: Air Flow and Cooling. AT&T has a full air conditioning and ventilation system at each GIDC to keep all data center elements working within normal operating temperatures.

COMPONENT	DESCRIPTION
HVAC	<ul style="list-style-type: none"> • Cooling towers and tanks supply water to chillers or plate heat exchangers. • Chillers or plate heat exchangers chill-supplied water down to 55°F. • Water pumps deliver the chilled water to pipes that travel under raised floor to CRAC units. • Chilled water inside the coil system cools air that is distributed under the raised floor and then up through vented floor tile. CRAC units are configured in N+1 redundancy.

Table 1.5.2.3-4: Air Conditioning and Ventilation. AT&T designs air conditioning and ventilation systems for GIDCs to keep hosted equipment at normal operating temperatures.

Agencies will benefit from the AT&T GIDC air conditioning and ventilation design by having their applications, and the associated hosting servers protected in suitable environmental conditions from detrimental heat.

1.5.2.3.a.4 Smoke Detection and Fire Suppression

Figure 1.5.2.3-5

displays the aspects of smoke detection and fire suppression in a GIDC, followed by **Table 1.5.2.3-5**, which discusses smoke detection and fire suppression in further detail.

Comprehensive physical security helps to protect Agency hosting equipment and applications from access

by unauthorized personnel. Agencies will benefit by knowing procedures are in place to secure hosting infrastructure and to make such equipment available for access by their end users and constituents.

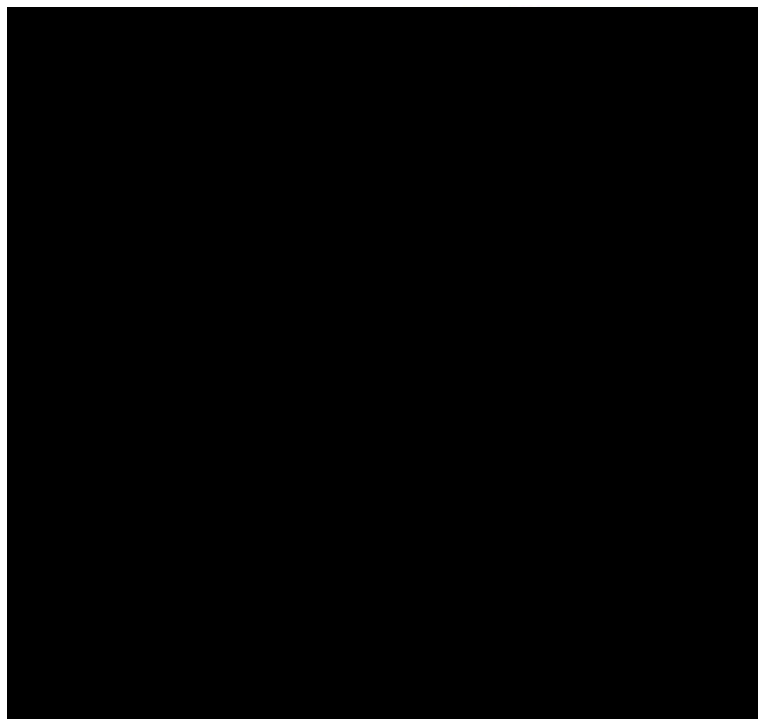


Figure 1.5.2.3-5: Smoke Detection and Fire Suppression. The GIDC smoke detection and fire suppression consists of dry pipe and VESDA systems.

COMPONENT	DESCRIPTION
Smoke Detection	<ul style="list-style-type: none"> • IDCs use a state-of-the-art VESDA smoke detection and alarm system.
Fire Suppression	<ul style="list-style-type: none"> • Data centers incorporate non-corrosive, pre-action dry pipe fire suppression system.

Table 1.5.2.3-5: Smoke Detection and Fire Suppression. *GIDCs use state-of-the-art smoke detection and fire suppression systems to protect the hosted environment from damage.*

The use of a highly sensitive smoke detection system, such as VESDA, will benefit Government Agencies by providing very early warning smoke detection, thus preventing smoke and fire damage. Agencies will also benefit from a dry pipe fire suppression system as the dry pipe system will fill with water, and the sprinkler heads will discharge water only in the affected areas of a GIDC, in the case of a fire.

1.5.2.3.a.5 Physical IDC Security

While AT&T’s data centers provide convenient access to authorized personnel, AT&T maintains some of the most comprehensive security measures in the industry. Access to network facilities is controlled through six levels of mandatory physical security, as described in **Table 1.5.2.3-6.**

SECURITY FEATURE	DESCRIPTION
Guards on premises 24x7	Security guards maintain the following procedures for allowing entry into the data centers: <ul style="list-style-type: none"> • For Agencies, contractors, repair personnel, and maintenance personnel, admission is granted by guard security. Access to buildings and critical areas is permitted at all times, provided there is an escort. • For guests of local employees, admission is granted by guard security. Access to buildings is permitted to guests of local employees during working hours, provided there is an escort. During nonworking hours, no admission to buildings or critical areas is permitted for local employee guests. At no time are guests of local employees permitted access to critical areas. • For vendors, admission is granted by guard security. Access to buildings and critical areas is permitted during working hours, provided there is an escort. No admission to buildings or critical areas is permitted for vendors during nonworking hours.
Person-traps located at each entry/exit point in data center	Physical mantrap doors are located at entry/exit point in the data center as part of the physical security.

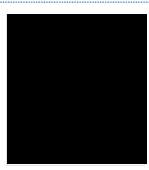

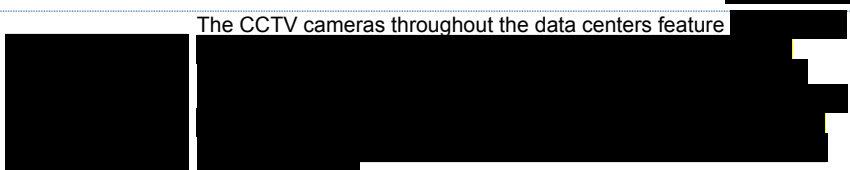
SECURITY FEATURE	DESCRIPTION
Card Key Reader (Electronic Badge)	 AT&T issues identification badges to all persons with a business need to access IDC premises. Admission is granted only by presentation of a valid ID badge. Access is granted either by an electronic badge reader or through passcode entry. Visitors are to be escorted either by an employee, resident, or guard while on IDC premises.
Biometric Palm Readers located at each entry/exit point in the data center	In addition to mantrap doors at an entry and exit point in the data center, biometric palm readers are an added line of physical security. 
Closed Circuit TV (CCTV) Monitor	The CCTV cameras throughout the data centers feature 
Cage/Cabinet Key	When not being actively worked in, all cabinets must be locked. This includes both front and back doors of the cabinets. At the beginning and end of each shift, the designated person(s) on duty needs to physically walk through all aisles of the data center to verify all cabinet doors are secure. Thus, cabinet doors are locked, even across shifts.
Alarms	<ul style="list-style-type: none"> • All entrances and exits to building and data center • Forced entry generates alarm at guard station and NOC • Tamper alarms generated by card readers

Table 1.5.2.3-6: IDC Physical Security. Agencies can take comfort knowing their hosting equipment is safe from tampering, based on the different levels of security in each IDC.

1.5.2.3.a.6 IDC Operations Centers

Domestically and globally, AT&T has incorporated into several of the IDCs an integrated NOC. Each NOC is staffed with experienced and trained personnel to monitor and manage the health of Agency hosting equipment, as well as the overall health of each IDC.

Using the integrated Global Enterprise Management Systems (iGEMS) at each NOC, technicians can proactively monitor Agency networking and computing systems. The iGEMS also allows AT&T technicians to provide 24x7 management of end-to-end Agency business-critical applications, along with provisioning, inventory, performance measurements, and capacity planning for Agency hosting environments.

1.5.2.3.b Attributes and Values of Service Enhancements

(b) If the offeror proposes to exceed the specified service requirements (e.g., capabilities, features, interfaces), describe the attributes and value of the proposed service enhancements.

In addition to the standard services, Agencies can enhance their CHS with additional features and capabilities for an additional fee. **Table 1.5.2.3-7** highlights additional service features and capabilities available with CHS. AT&T proposes the attributes in **Table 1.5.2.3-7** as service enhancements.

FEATURE	DESCRIPTION	BENEFIT
[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]

FEATURE	DESCRIPTION	BENEFIT
[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]

Table 1.5.2.3-7: Service Enhancements. [REDACTED]

Agencies can subscribe to a combination of the optional service enhancements. The benefits these services will bring to Agencies include ease of transition, application and network optimization, and enhanced application and network security.

1.5.2.3.c Service Delivery Network Modifications

(c) Describe any modifications required to the network for delivery of the services. Assess the risk implications of these modifications.

Agencies receive a low-risk solution through AT&T’s ability to offer CHS upon contract award, without modifications to the network or operational support systems.

1.5.2.3.d Management and Applications Services Experience

(d) Describe the offeror’s experience (including major subcontractors) with delivering the mandatory Management and Applications Services described in Section C.2 Technical Requirements.

AT&T Networkx Team offers Agencies extensive experience providing managed services that create value to our customers in Government and commercial entities. This experience has given us the ability to engineer and deliver services. Two examples of AT&T Team’s ability to deliver managed services are listed in **Table 1.5.2.3-8**.

LARGE INTERNET TRAVEL SERVICES PROVIDER		
Client Need	Solution	Created Value
[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]

Table 1.5.2.3-8: Experience Delivering Managed Services. Success is measured by the ability to deliver solutions to Agencies that create value to their business.

As evidenced by **Table 1.5.2.3-8**, AT&T has extensive experience and history in providing CHS to commercial and Government entities. With such experience, AT&T will be able to provide the same, high-quality CHS to Agencies under the Networx contract.

1.5.2.3.e Approach to Network Infrastructure Management

(e) For Managed Network Services (MNS), describe the approach, process, and considerations for managing a network infrastructure (e.g., FRS, ATMS, IPS, IP-VPNs, CPE) supporting approximately 2000 users, at 25 locations across the United States. Based on the offeror's experience with similar projects, provide a discussion of how the offeror would investigate the requirements, design the solution, implement the plan, and deliver service that meets the Agency's performance requirements.

The approach, process, and considerations for network infrastructure management are described in Section 1.5.6.3.e.

1.5.2.4 Narrative Text Requirements

1.5.2.4.1 The IDC shall support the following capabilities: [C.2.4.3.1.4]

Security (Building and Facilities)

The contractor shall describe the offered security methods and procedures.

A detailed discussion of the physical security protecting collocation space is described in Section 1.5.2.3.a.5.

1.5.2.4.2 The IDC shall support the following capabilities: [C.2.4.3.1.4]

Network Connectivity and Bandwidth

The contractor shall describe its Internet infrastructure (e.g., Tier-1 backbone connectivity) – or business relationships with other Network Service Providers – that ensure minimal latency, fewest possible Autonomous System hops, et cetera.

Agency applications and servers using CHS will be hosted in AT&T IDCs, which have direct redundant OC-48 connections to AT&T's Internet backbone with optional peering connections to other Tier 1 ISPs. A detailed discussion on AT&T's IP backbone network and peering arrangements is described in Section 1.3.2.b.

Along with the Internet infrastructure discussion in Section 1.4.6, AT&T offers optional services for the ISP routing services from an IDC perspective (**Table 1.5.2.4-1**).

FEATURE	DESCRIPTION
Multi-ISP Services	Provides end users with multi-homed front-end connectivity within U.S. IDCs
BGP Routing Services	Provides support or fully-managed solution when combined with dedicated multi-ISP services for BGP routing clients that are multi-homing

Table 1.5.2.4-1: Multi-ISP Features. Agencies are provided several options for multi-ISP connections into an AT&T GIDC.

Agencies can benefit from the different multi-ISP features by incorporating a second ISP connection for redundancy or disaster recovery, thus providing maximum uptime to their servers and applications.

1.5.2.5 Stipulated Deviations

AT&T takes neither deviation nor exception to the stipulated requirements.

1.5.2.6 Government Provided Rack Features

1.5.2.6.1 Vendor Data Center

AT&T will provide the Internet data center (IDC) for CHS service and allow Government Agencies to provide their own equipment contingent upon AT&T approval for install and use in the AT&T IDC environment. Based on the number of racks and equipment that an Agency provides, the proper amount or square footage, power and HVAC will be provided by AT&T. The data center environment includes power, heating, ventilation and air conditioning (HVAC), infrastructure/infrastructure maintenance and security. AT&T will provide a Colocation environment in accordance with its standard operating procedures.

Power

Each IDC has Uninterruptible Power Supply (UPS) systems. UPS systems receive power from both the commercial power utility and the standby generators. Each UPS system conditions the power and feeds the conditioned power to redundant power distribution units (PDUs). In case of a commercial power failure, multiple standby generators are available to provide power to the IDC [REDACTED]

[REDACTED]

HVAC

Computer Room Air Conditioning (CRAC) units are strategically placed in the IDC to assure the appropriate ambient temperature thresholds are met. [REDACTED]

[REDACTED]

Infrastructure/Infrastructure Maintenance

All scheduled maintenance on common infrastructure is scheduled during known maintenance windows and must be reviewed by an AT&T Subject Matter Experts (SMEs) using Service Method of Procedure process (SMOP).

[REDACTED]

[REDACTED] This applies to all Network, power, and facilities infrastructure.

Physical Security of the IDC

Security includes controlled access and egress doors, controlled access permissions and access request methods, and managed key and /or access card plans for access control. CCTV cameras are used to monitor access, egress, and infrastructure. Common infrastructure areas are secured areas. AT&T will attempt to provide off street parking, where feasible, with adequate lighting. AT&T is not liable for damage, loss, or theft of vehicles, and/or contents thereof.

Power Draw

Agency CHS configurations require adherence to a Maximum Power Draw value for the Agency CHS space. [REDACTED]

[REDACTED]

The following requirements apply to power circuits ordered by an Agency:

- AT&T requires all circuits be ordered with one, (1) primary and one, (1) redundant circuit for fail-over per cabinet or rack.
- The aggregate draw for power circuits ordered by customer shall not exceed [REDACTED] in the customer's cage area.

If the Customer's actual power requirement exceeds [REDACTED] [REDACTED] customer may purchase additional contiguous space to accommodate power consumption and heat dissipation. [REDACTED]

[REDACTED]

An Agency's CHS environment will be metered for power usage. [REDACTED]

[REDACTED]

1.5.2.6.1.1 AT&T IDC Guidelines for Government Furnished Equipment

The following section lists AT&T IDC guidelines for Government Furnished Equipment placed in an AT&T IDC:

Government Provided Rack

Agencies may provide their own racks or cabinets upon approval [REDACTED]
[REDACTED] The dimensions and height of the Agency
provided cabinet must be listed [REDACTED]
[REDACTED]
[REDACTED]

Web Cams

Web cams are permissible as long as they are fixed-mount placements
without pan-tilt-zoom capabilities. The field of view must be limited to
Agency's cage floor space ONLY. [REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

Environmental Sensing Devices

Should Agency install environmental sensing devices in their cage or
cabinet, the readings obtained [REDACTED]
[REDACTED]

Government Furnished Power Strips

Agencies may use their own metered power strips. [REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

[REDACTED]

Government Furnished Additional Security Devices

[REDACTED]

1.5.2.6.2 Vendor Install

An additional offering to the CHS features will be vendor installation of a Government provided rack. An Agency will be responsible for providing the proper number of racks and all associated installation hardware t [REDACTED]

[REDACTED]

1.5.2.6.3 Custom Power

As each Agency colocated hosting configuration varies, power above and beyond the standard [REDACTED]

[REDACTED]

1.5.2.7 POP-Based Collocation Hosting Service

When recommended by AT&T to fulfill Agency service requirements, AT&T may provide Collocated Hosting Service [REDACTED]. [REDACTED] AT&T provides Collocation Hosting Service at the AT&T Internet Data Centers (IDC).

1.5.2.7.1 Capabilities

[REDACTED] CHS supports the standards defined for the CHS service as specified in section C.2.4.3.1.2 of the Networkx Universal requirements document.

[REDACTED] CHS supports the connectivity defined for the CHS service as specified in section C.2.4.3.1.3 of the Networkx Universal requirements document.

[REDACTED] CHS supports the technical capabilities defined for the CHS service as specified in section C.2.4.3.1.4 of the Networkx Universal requirements document.

[REDACTED] CHS supports the features defined for the CHS service as specified in section C.2.4.3.2 of the Networkx Universal requirements document.

[REDACTED] CHS supports the interfaces defined for the CHS service as specified in section C.2.4.3.3 of the Networkx Universal requirements document.

[REDACTED] CHS supports the performance metrics defined for the CHS service as specified in section C.2.4.3.4 of the Networkx Universal requirements document.

1.5.2.7.2 Service Locations

[REDACTED] CHS is only offered in CONUS locations where there is available space within an AT&T POP facility.