1.5.1 Dedicated Hosting Services (DHS) [C.2.4.2]

Agencies will fulfill e-Gov and Federal Enterprise Architecture (FEA) initiatives, and implement critical applications with a fully compliant Dedicated Hosting Service (DHS) that meets the highest standards in reliability, security, scalability, and global reach. A low-risk DHS is 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.

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

1.5.1.1.a Approach to Service Delivery [L.34.1.5.1.a]

(a) Analyze the service requirements specified in this solicitation and describe the approaches to service delivery for each service. [L.34.1.5.1.a]

Agencies will benefit from a high-availability service, layered security (physical and electronic) and scalable IP connectivity, providing Agencies with the best quality, lowest latency, and secure environments.

AT&T's Enterprise Hosting Services (EHS) is a continuum of hosting and management capabilities that provides Agencies with a global, scalable, reliable, and flexible infrastructure for running their e-business applications. As a component of EHS, DHS provides an array of hosting and management services designed to allow Agencies to outsource enterprise-class e-business applications that address their needs and challenges. **Figure 1.5.1.1-1** displays this continuum of hosting and management capabilities.

[redacted]

Figure 1.5.1.1-1: Continuum of Hosting and Management Services. *Agencies will be able to implement enterprise class e-business applications that address the Agencies' hosting requirements, through a number of management and hosting options from a single enterprise hosting umbrella.*

A tiered managed solution offers Agencies flexibility to choose a low-risk DHS solution that will exceed Agency-specific service requirements, such as applications including Oracle and Microsoft SQL. **Figure 1.5.1.1-2** depicts these elements in the overall DHS architecture, as well as detailing other elements in the service.

Agencies can rely on AT&T to provide a globally available and secure DHS that will exceed with the Government's requirements. **Table 1.5.1.1-1** discusses the approach to service delivery of a DHS solution.

[redacted]

Figure 1.5.1.1-2: DHS Architecture. *Agencies can take advantage of the available service elements to create a high availability and secure DHS solution.*

SERVICE DELIVERY APPROACH	DESCRIPTION
Operate Internet Data Centers (IDCs) under defined physical and security standards	N+1 Redundancy *IDC* [redacted] *IDC Physical* [redacted] *IDC Logical Security* [redacted] *IDC Air Conditioning* [redacted] *IDC Smoke Detection and Fire Suppression* [redacted]
Provide facilities-based IDCs and interconnect to the leading Tier 1 Internet service provider (ISP)	• AT&T owns, operates, and manages all IDCs and facilities [redacted] • Extensive pr vate peering arrangements with other ISPs [redacted]
Provide a Tiered Managed Solution	AT&T provides tiers of management based on Agency requirements: • *AT&T Managed* - AT&T provisions, installs, monitors, manages, maintains, and reports on certified applications operating systems, and hardware. AT&T-managed capabilities allow clients to buy hosting services as a set of individually configured and managed components. • *AT&T Enhanced Managed* - AT&T provisions, installs, and provides application performance management and comprehensive reporting. AT&T enhanced managed capabilities are available for clients who want to buy an end-to-end integrated hosting solution, where the entire solution is configured to meet their business and performance objectives.
Provide Flexible Service Offerings	Agency outsourcing of their hosting requirements will be poss ble by being provided a feature-rich DHS service, including: [redacted]
Integrate with Security Services	Agency hosting service is protected from the public domain through: • Managed Firewall Services • Managed Intrusion Detection • Vulnerability Scanning

Table 1.5.1.1-1: Service Approach. *Agencies can subscribe to a DHS that will be delivered with high availability, reliability, and security.*

DHS will provide Agencies with a high availability and secure hosting environment, along with management options to best suit an Agency's specific hosting and management requirements.

1.5.1.1.b Benefits to Technical Approach [L.34.1.5.1.b]

(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). [L.34.1.5.1.b]

AT&T's Networx services, in general, and DHS, 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 1.5.1.1-2** 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 IDCs 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 and secure environment for their applications hosted on DHS facilities.	As a component of Technical Reference manual (TRM)/service platform and infrastructure/hardware/infrastructure, Agencies can be secure that their web, media, and application servers are safely located in a reliable, disaster-tolerant hosting environment.
Provide Facilities-based IDCs and interconnect to the 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 superior end-to-end 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 Tiered Managed Solution	Agencies can tailor a solution to fit their hosting, network, and management requirements.	As a component of TRM/service access and delivery/service transport, Agencies can reduce cost overruns by contracting to only the DHS elements they require.
Provide Flex ble Service Offerings	Agencies can design a robust, flexible hosting service to comply with requirements.	As a component of TRM/service access and delivery/service requirements, Agencies can save costs by customizing their hosting service and subscribe to only required hosting elements.
Integrate with Security Services	Agencies can protect their hosting environment from unauthorized access from the public domain.	As a component of TRM/component framework/security, Agencies can feel secure knowing their hosting servers and applications are protected from disruptions resulting in possible cyber attacks.

Table 1.5.1.1-2: 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:

- Technical Reference Model (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 can assist specific departments and Agencies to meet mission and business objectives through a comprehensive DHS offering.

1.5.1.1.c Major Issue to Service Delivery [L.34.1.5.1.c]

(c) Describe the problems that could be encountered in meeting individual service requirements, and propose solutions to any foreseen problems. [L.34.1.5.1.c]

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 1.5.1.1-3 lists the top seven service delivery risks and our mitigation strategy [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]

RISKS	RISK DESCRIPTION	RISK MITIGATION
Requirements Changes	Requirements changes before and after service delivery contributes to budget overruns, schedule slips, and missed expectations.	[redacted]
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 1.5.1.1-3: AT&T Service Delivery Lessons Learned and Risk Mitigation Strategies. *Agencies benefit from lessons learned and experience implementing DHS, which ultimately minimizes service delivery risks.*

AT&T has taken steps to identify risk and provide risk mitigation associated with delivering DHS. 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.

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

1.5.1.2.a Service Quality and Performance [L.34.1.5.2.a]

(a) Describe the quality of the services with respect to the performance metrics specified in Section C.2 Technical Requirements for each service. [L.34.1.5.2.a]

As a DHS provider, AT&T strives to meet and exceed common industry performance levels for managed hosting. Agencies will receive a high quality

DHS that meets the performance levels and acceptable quality level (AQL) of key performance indicators (KPIs) for DHS, as presented in the RFP and in **Table 1.5.1.2-1**.

KEY PERFORMANCE INDICATOR (KPI)	USER TYPE	PERFORMANCE STANDARD (THRESHOLD)	PROPOSED SERVICE QUALITY LEVEL
Availability (Internet Connection)	All	99.99%	[redacted]
Availability (Website)	Routine	99.7%	[redacted]
Time to Restore (TTR)	Without Dispatch	4 hr	[redacted]
	With Dispatch	8 hr	
[redacted]			

Table 1.5.1.2-1: DHS Performance Parameters. *Agencies receive a high quality DHS through support and compliance with DHS KPIs listed in the table above.*

With the Networx contract, one of AT&T's priorities is to provide Agencies with a superior DHS offering. By meeting the AQLs for the specified KPIs, AT&T will provide Agencies with a high-availability network and DHS.

1.5.1.2.b Approach to Monitoring and Measuring Performance [L.34.1.5.2.b]

(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. [L.34.1.5.2.b]

Identifying KPIs is a key component to providing a high level of service. Of equal importance are the methods for capturing, measuring, and monitoring the identified KPIs. For each KPI associated with DHS, AT&T has a methodology for measuring and monitoring. **Table 1.5.1.2-2** describes the approach for monitoring and measuring the KPIs, as listed in this section by the Government.

[redacted]

KEY PERFORMANCE INDICATOR	APPROACH TO MEASURING AND MONITORING
Availability (Internet Connection)	[redacted]
Availability (Website)	[redacted]
Time to Restore (TTR)	[redacted]

Table 1.5.1.2-2: Monitoring and Measuring Performance. *Agencies will meet KPI requirements, based on tried and true methodologies for monitoring and measuring performance.*

Performance data that is collected through iGEMS is presented in the AT&T Managed Portal Service Dashboard, which comprises several views from which Agencies can choose. **Table 1.5.1.2-3** describes several of the Dashboard options.

REPORTING	REPORT NAME	REPORT DEFINITION
Performance	[redacted]	[redacted]
	[redacted]	[redacted]
Acceptable Quality Levels (AQL)	[redacted]	[redacted]
	[redacted]	[redacted]

Table 1.5.1.2-3: iGEMS Dashboard Options. *Agencies can use a user-friendly interface to obtain* [redacted] *performance metrics.*

Agencies benefit from AT&T's approach to monitoring and measuring the DHS KPIs by having comprehensive methods and procedures. Such methods and procedures provide Agencies a clear definition of service performance.

1.5.1.2.c Approach to Perform Service Delivery Verification [L.34.1.5.2.c]

(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. [L.34.1.5.2.c]

The first time the service is provided through the Networx contract, the service performance must be verified; KPIs will be monitored to certify that the service performance complies with the AQL. **Table 1.5.1.2-4** summarizes the verification and testing procedures for the DHS KPIs.

KEY PERFORMANCE INDICATOR	VERIFICATION APPROACH	TESTING PROCEDURES
Availability (Internet Connection)	[redacted]	[redacted]
Availability (Website)	[redacted]	[redacted]
Time to Restore (TTR)	[redacted]	[redacted]

Table 1.5.1.2-4: Service Delivery Verification. [redacted]

To simplify the verification process, AT&T has automated the process. [redacted] The service verification process is presented in greater detail in Section 1.3.2.d, Approach to Perform Service Delivery Verification.

1.5.1.2.d Performance Level Improvements [L.34.1.5.2.d]

(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. [L.34.1.5.2.d]

The performance characteristics of AT&T's hosting facilities, combined with high-capacity network connectivity, create a high-performance hosting service [redacted]

Table 1.5.1.2-5 lists the key availability and performance targets, as compared to the RFP performance targets.

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

Table 1.5.1.2-5: Performance Level Improvements. [redacted]

For DHS designed with ISP diversity and high-availability web server design, Agencies will receive improved availability and minimal downtime. The combination of a high-capacity network and performance characteristics of AT&T's hosting facilities provides a service whose performance levels meet or exceed the AQLs, as stated in the RFP.

1.5.1.2.e Approach and Benefits for Additional Performance Metrics [L.34.1.5.2.e]

(e) Describe the benefits of, and measurement approach for any additional performance metrics proposed. [L.34.1.5.2.e]

The KPIs defined by the Government for DHS will provide a comprehensive assessment for service verification and service performance monitoring. [redacted]

1.5.1.3 Satisfaction of Management and Applications Service Specifications [L.34.1.5.3]

1.5.1.3.a Service Requirements Description [L.34.1.5.3.a]

(a) Provide a technical description of how the service requirements (e.g., capabilities, features, interfaces) are satisfied. [L.34.1.5.3.a]

AT&T's DHS offering consists of a number of components starting with the equipment architecture of an IDC, as depicted in **Figure 1.5.1.3-1**.

Table 1.5.1.3-1 provides a narrative of the equipment architecture and other components of the DHS offering.

[redacted]

Figure 1.5.1.3-1: IDC Architecture. *Agency applications achieve superior uptime through N+1 redundancy, and carrier-class hardware from leading vendors.*

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.

SERVICE REQUIREMENTS	DESCRIPTION	BENEFITS TO AGENCY
	[redacted]	
Internet Front End Connectivity	[redacted]	Agencies will have high-speed connectivity to the Internet for their managed hosted environment.
Monitoring and management capabilities	AT&T offers several monitoring and management options, based on the management tier (AT&T Managed, AT&T Enhanced Managed). These are listed below: [redacted] [redacted] [redacted]	Agencies can subscr be to different monitoring and management options, receiving increased performance management and improved service levels, compared to the standard DHS offering.
DHS/GIDC Environment	GIDC architecture consists of over two million square feet of combined space in North/South America and Continental Europe. GIDC environment consists of three elements: • Commercial and backup power • Air conditioning and ventilation • Smoke detection and fire suppression [redacted]	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 DHS facilities.
Hardware (HW)/Software (SW)/Operating System (OS) types and vendors	• Server options [redacted] [redacted] OS options [redacted] • SW options [redacted] Software comes in two categories: AT&T certified and installed. • **AT&T Certified Software –** AT&T Certified Software is operating system and application software for which AT&T can provide Advanced Monitoring, Advanced Management, or Performance Management Services. AT&T installs and maintains certified software and works with software vendors on trouble reporting and resolution and can license the software or the client can purchase the license directly. • **Installed Software –** Installed software is software that AT&T will place on a certified server.	Agencies can choose from an a la carte list of common hosting HW, SW, and OS platforms, which is certified and easily managed and monitored by AT&T.
Managed Firewall (FW) Service	Managed FW services provide the HW and management of the FW(s) in an AT&T IDC. FW hardware (HW) supported are the following: [redacted] • [redacted]	Agencies can choose the firewall service that best satisfies their requirements, and also provides a first line of defense to protect the Agency's network and applications from unauthorized access.
Managed Threat Protection Services	Managed Threat Protection Services provide an extra layer of protection beyond Managed FW Services by providing intrusion detection services (IDS). The different IDS options are listed below: • Network Based Intrusion Detection System (NIDS) • Host Based Intrusion Detection System (HIDS) • Advanced Network Based Intrusion Detection Service (ANIDS) • Advanced Host Based Intrusion Detection Service (AHIDS)	Protects Agencies' mission-critical systems from disruption by a malicious attacker or an unauthorized event and provides security with around-the-clock surveillance of network and

SERVICE REQUIREMENTS	DESCRIPTION	BENEFITS TO AGENCY
		applications from unwanted access and events.
IT Security and Security Consulting	IT Security – [redacted]	Provides Agencies with vulnerability scanning and recommendations on further securing their DHS environment.
Managed Load Balancing Services	Balances web traffic across client's multiple servers. Both single location and multi-location load balancing services are available. • Local Load Balancing balances traffic across multiple servers within a single data center • Local Load Balancing High Availability balances traffic across multiple servers within a single data center, while providing load balancing switch redundancy • Global Load Balancing between two AT&T GIDCs or between an AT&T GIDC and a client premise balances traffic between multiple websites and servers in two geographically diverse locations	Agencies benefit by reducing the threat of network overloads and server and application failures by optimally distr buting Agency traffic to provide responsive, satisfying experiences for their end users and constituents.
Restoration	AT&T Tape Back-up and Restore (TB&R) Service provides an Agency with the ability to save files on tape for the purpose of later restoring them, if needed. Backup Cycle: Automated backup of client-defined file systems and DB files consists of: [redacted]	Agencies can be secure knowing they will always have a backup of files
Web Reporting	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: [redacted]	Agencies can view their managed hosted environment metrics through a web portal at anytime.

Table 1.5.1.3-1: Service Description. *A wide range of technical components is available to help Agencies develop a failsafe, managed DHS offering.*

Inclusive of the components in the above table, the following narratives provide additional details of the components that encompass DHS, including the overall hosting network, power architecture, air conditioning, smoke detection and fire suppression, and physical IDC security.

1.5.1.3.a.1 Hosting Network

All IDCs are located either with an Internet gateway node or a backbone node, as depicted in **Figure 1.5.1.3-2**, providing for high-speed access from the DHS directly to AT&T's IPS backbone or another ISP through a gateway node. DHS facilities span worldwide, as listed in **Table 1.5.1.3-2**.

[redacted]

Figure 1.5.1.3-2: Global IDC Locations. *Agencies will have high speed access to the Internet from all IDCs as all IDCs are located with an Internet gateway node or backbone node.*

[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]

Table 1.5.1.3-2: Worldwide DHS Facilities. *AT&T DHS facilities have worldwide coverage.*

AT&T's worldwide DHS facility coverage provides Agencies the benefit of deploying applications to reach global users. Deploying Agency applications closer to the end users will provide them better overall user experience.

1.5.1.3.a.2 Power Architecture

Figure 1.5.1.3-3 depicts the aspects of commercial and backup power and power conditioning in a GIDC, followed by **Table 1.5.1.3-3**, which discusses the GIDC power architecture in further detail.

[redacted]

[redacted]

Figure 1.5.1.3-3: GIDC Power Architecture. *Agency-hosted equipment and applications benefit from a redundant power architecture that provides superior uptime.*

The redundant power architecture, within an IDC, will benefit Agencies with no interruption to their hosting infrastructure and applications in the case of commercial power failure. Thus, end users and constituents will not experience any ill effects on their ability to reach a certain Agency application or website.

COMPONENT	DESCRIPTION
DHS/Global IDC (GIDC) power	All GIDCs are facilities-based, meaning AT&T owns all the physical infrastructure. Inclusive of the physical environment are the following:

COMPONENT	DESCRIPTION
architecture	• *Power Handling* [redacted] • *Diesel Power Generation*: [redacted] • [redacted] • *Conditioned Power*: [redacted] • *Power Distribution Units (PDU)*: [redacted] • *Remote Power Panels*: [redacted] • Grounding Architecture: [redacted]

Table 1.5.1.3-3: GIDC Power Architecture. *Agency-hosted applications benefit from a hosting service that is highly redundant and highly available.*

1.5.1.3.a.3 Computer Room Air Conditioning

Proper ventilation is vital to the stability of DHS servers. **Figure 1.5.1.3-4** displays the different elements that are part of a GIDC air conditioning system. **Table 1.5.1.3-4** discusses the details of air conditioning for a GIDC.

[redacted]

Figure 1.5.1.3-4: 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
Heating, Ventilation and Air Conditioning (HVAC)	• Cooling towers and tanks supply water to chillers or plate heat exchangers • Chillers or plate heat exchangers chill the 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, which is distributed under the raised floor and then up through vented floor tile. CRAC units are configured in N+1 redundancy.

Table 1.5.1.3-4: 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 environmental conditions from detrimental heat.

1.5.1.3.a.4 Smoke Detection and Fire Suppression

Figure 1.5.1.3-5 displays the aspects of smoke detection and fire suppression in a GIDC, followed by **Table 1.5.1-5**, which discusses smoke detection and fire suppression in further detail.

[redacted]

Figure 1.5.1.3-5: Smoke Detection and Fire Suppression. *The GIDC smoke detection and fire suppression consists of dry pipe and VESDA systems.*

COMPONENT	DESCRIPTION
Smoke Detection	• IDCs use a state-of-the-art VESDA smoke detection and alarm system. [redacted] • Conventional smoke detectors are also used and grouped into zones.
Fire Suppression	• Data Centers incorporate a noncorrosive, pre-action dry pipe fire suppression system. [redacted]

Table 1.5.1.3-5: 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.

1.5.1.3.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 1.5.1.3-6**.

SECURITY FEATURE	DESCRIPTION
Guards on premises 24x7	Security guards maintain the following procedures for allowing entry into the data centers: • 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 non-working 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 non-working hours.
Mantraps 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. [redacted]
Card Key Reader (Electronic Badge)	[redacted] AT&T issues identification badges to all persons having a business need to access IDC premises. Admission is granted only by presentation of a valid ID badge. Access is granted either by a 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 data center	In addition to person-trap doors at each entry and exit point in the data center, biometric palm readers are present as an added line of physical security. [redacted]

SECURITY FEATURE	DESCRIPTION
Closed Circuit TV (CCTV) Monitor	CCTV cameras located throughout the data centers feature [redacted]
Cage/Cabinet Key	When not being actively worked in, all cabinets must be locked. This includes both the front and back doors of the cabinets. [redacted]
Alarms	[redacted]

Table 1.5.1.3-6: IDC Physical Security. *Agencies can take comfort knowing AT&T helps protect their hosting equipment from tampering, based on the different levels of security in each IDC.*

Comprehensive physical security helps protect Agency hosting equipment and applications from access by non-authorized personnel. Agencies will benefit by knowing their hosting infrastructure is protected and their websites/applications are available for access by their end users and constituents.

1.5.1.3.a.6 IDC Operations Centers

Domestically and globally, AT&T has incorporated into the IDCs an integrated network operations center (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 System (iGEMS) at each NOC, technicians can proactively monitor Agency networking and computing systems. Also, iGEMS 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.

1.5.1.3.b Attributes and Values of Service Enhancements [L.34.1.5.3.b]

(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. [L.34.1.5.3.b]

In addition to the standard services, Agencies can enhance their DHS with additional features and capabilities for an additional fee. **Table 1.5.1.3-7** highlights additional service features and capabilities available with DHS. AT&T proposes the attributes in **Table 1.5.1.3-7** as service enhancements.

FEATURE	DESCRIPTION	BENEFIT
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]

FEATURE	DESCRIPTION	BENEFIT
	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]

Table 1.5.1.3-7: 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, optimization of applications and networks, and enhanced applications and network security.

1.5.1.3.b.1 Dedicated Hosting Reporting

AT&T views reporting as a key differentiator to our service and provides many different and customizable reports (Appendix H, Table H.1-1) through our AT&T **Business**Direct that will make any Agency hosting project a success.

1.5.1.3.c Service Delivery Network Modifications [L.34.1.5.3.c]

(c) Describe any modifications required to the network for delivery of the services. Assess the risk implications of these modifications. [L.34.1.5.3.c]

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

1.5.1.3.d Management and Applications Services Experience [L.34.1.5.3.d]

(d) Describe the offeror's experience (including major subcontractors) with delivering the mandatory Management and Applications Services descr bed in Section C.2 Technical Requirements. [L.34.1.5.3.d]

AT&T Networx Team offers Agencies extensive experience providing managed services that create value to our customers to both in Government and commercial entities. This experience has given us the ability to engineer and deliver services. Three examples of AT&T Team's ability to deliver managed services are listed in **Table 1.5.1.3-8**.

[redacted]

Client Need	Solution	Created Value
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]

[redacted]

Client Need	Solution	Created Value
[redacted]	[redacted]	[redacted]

Table 1.5.1.3-8: Experience Delivering Managed Services. [redacted]

As evidenced by **Table 1.5.1.3-8**, AT&T has extensive experience and history in providing DHS to commercial and Government entities. With such experience, AT&T will be able to provide the same, high-quality DHS to Agencies under the Networx contract.

1.5.1.3.e Approach to Network Infrastructure Management [L.34.1.5.3.e]

(e) For Managed Network Services (MNS), descr be 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 Unites 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. [L.34.1.5.3.e]

For a detailed description of AT&T's methodologies on requirements gathering and solution design and implementation and delivery of managed network services, refer to Section 1.5.6.3.e, Managed Network Services.

1.5.1.4 Narrative Text Requirements

The AT&T Networx Team approach to delivering application hosting is to use the core capabilities within the DHS offerings, while leveraging AT&T's and AT&T Networx partner's key capability to design, deploy, and manage complex hosted applications. AT&T has selected leading industry-managed application service providers as strategic partners. These strategic partners, along with AT&T as the lead, will develop custom application solutions, based on Agency requirements to support the Agency's overall mission.

1.5.1.4.1 Customer Relationship Management (CRM) Application Hosting [C.2.4.2.2.1 (4)]

Application Hosting [Optional]
The contractor (i.e. Application Service Provider [ASP]) shall provide hosted applications including but not limited to: *Customer Relationship Management (CRM)* for the management of government's relationship with its constituents. At present, CRM systems are only partially relevant in the public sector. In future, federal Agencies may increasingly adopt best private sector practices regarding customer care and support.

Designing, deploying, managing, and evolving Agencies Customer Relationship Management (CRM) solutions require skilled networking professionals, rigorous processes, and sophisticated tools. AT&T, with our strategic partners, will help deliver predictable CRM performance, with a real-time view into that performance. CRM solutions, such as Siebel, are a way to become a mission-driven Agency. Designing, deploying, managing, and evolving a high-performing CRM application and network infrastructure focuses on:

- Data and query security to protect sensitive information
- Availability and performance visibility for meeting Agency objectives
- Resources, processes, and tools need to maintain and introduce change into the application and its infrastructure
- Capacity to support data volumes
- Database integrity, availability, and performance
- Access methods and reach for the Agency and the Agency's partners
- Network infrastructure bandwidth to support the Agency users' community size and query volume.

AT&T's application performance management integrates with the Agencies' CRM application and network infrastructure across network, systems, and appliction (**Figure 1.5.1.4-1**). AT&T provides Agencies with confidence that transactions and queries reach the application, and that they are processed and results are returned to the end user.

AT&T' uses time-tested, proven processes to provide predictable performance. Those processes include application due diligence and stress testing, service level and configuration engineering, configuration and inventory management, and finally, installation and configuration testing.

[redacted]

Figure 1.5.1.4-1: AT&T Application Performance Management. [redacted]

Working with the Agency IT department and the Agency's end users to discover performance requirements, AT&T selects the parameters to monitor and set thresholds. Leveraging AT&T's application management structure, AT&T deploys a combination of intelligent probes and AT&T developed network node modules to monitor the CRM application. Once the CRM solution is deployed, AT&T's tools automatically detect when a parameter's performance approaches its threshold, generates an alarm and assigns a severity, and routes it to the appropriate support team. The alarm will also include a probable root cause and an action to take, enabling the support team to rapidly address the source of the problem.

To provide Agency visibility, AT&T provides a managed services portal (**Figure 1.5.1.4-2**) to provide access to report parameters and trouble tickets. The management service portal is available 24x7 and configurable to support different views, based on functional role of the end user.

[redacted]

Figure 1.5.1.4-2: AT&T Application Performance Reporting [redacted]

Only AT&T's Networx Team has the ability to inextricably link CRM applications with network infrastructure to map performance requirements to a networked environment. AT&T's Networx Team has the expertise to design, deploy, and manage custom CRM applications.

1.5.1.4.2 Database Systems Application Hosting [C.2.4.2.2.1 (4)]

Application Hosting [Optional]
The contractor (i.e. Application Service Provider [ASP]) shall provide hosted applications including but not limited to: *Database Systems* for management of large-scale, structured sets of data; supporting ad hoc query facilities; and, providing report generation capabilities

Aligned with strategic partners, AT&T will provide database management services (DBMS), offering Agencies a feature set for managing their database systems. [redacted]

The following database tools are available to Agencies for working with their databases through [redacted]:

[redacted]

[redacted]

[redacted] database management provides Agencies with the following management solutions:

[redacted]

[redacted] provide mature and reliable management systems that combine high levels of performance and availability. Both database management systems can handle a wide range of different types of information, making them suitable database management systems for diverse application scenarios.

1.5.1.4.3 Document Management Application Hosting [C.2.4.2.2.1 (4)]

Application Hosting [Optional]
The contractor (i.e. Application Service Provider [ASP]) shall provide hosted applications including but not limited to: *Document Management* including library services and management of workflow and collaboration.

AT&T's Document Management System is a complete enterprise solution for managing all corporate information from creation through ultimate destruction or preservation. AT&T's Document Management System has been developed to provide organizations with a commercial off-the-shelf (COTS) hosted solution for document management, workflow, imaging, and records management.

AT&T's Document Management System keeps corporate information safe and secure with security and access controls that are U.S. Department of Defense 5015.2-STD certified. AT&T's Document Management System's architecture is designed to support a distributed organization and scale, as required. An effective information management system must capture, register, organize, preserve, and make data available to all the people who need access to it. As information needs to be accessed by different groups of people, for different purposes, it is imperative that the information system be able to deliver relevant information to each group in a timely manner. The system has been developed with these requirements.

The system combines elements from virtually every document management technology to accommodate the needs of different groups. It is designed to accommodate information management for a distributed organization and provide fast response times in an efficient manner, while helping to protect data integrity.

[redacted]

1.5.1.4.4 E-mail/Messaging Application Hosting [C.2.4.2.2.1 (4)]

Application Hosting [Optional]
The contractor (i.e. Application Service Provider [ASP]) shall provide hosted applications including but not limited to: *E-mail/Messaging* Leading E-mail/Messaging software is increasingly the target of malicious programming and unauthorized use. Many organizations are turning to ASPs in order to mitigate the security risks associated with electronic mail. ASPs offer advanced and up-to-date security managements systems and procedures

AT&T's Enterprise Messaging Service (EMS) offers a total managed messaging solution, based on [redacted], and provides packages and optional features that will allow businesses to fulfill their messaging needs. The standard configuration of EMS can provide higher service levels, lower costs to internal IT departments, and a more variable cost structure that is predictable, based on number of mailboxes.

EMS also offers higher security availability and provides internal IT departments more time to focus on strategic initiatives. EMS also provides a flexible, scalable, reliable, and secure architecture. [redacted] EMS becomes a highly automated infrastructure to which other applications can be easily added.

The EMS standard configuration protects and supports mission-critical servers and applications in our world-class IDCs. The service includes redundant Internet access, 24/7 facilities monitoring, and access to our portfolio of managed messaging services, ensuring an uninterrupted business presence and the highest levels of performance, security, and reliability. **Figure 1.5.1.4-3** [redacted]

[redacted]

Figure 1.5.1.4-3: AT&T Enterprise Messaging Service. [redacted]

Agencies will benefit from AT&T's EMS by leveraging the strength of experienced technical and consulting staff, eliminating the need to recruit, train, and retain qualified experts. [redacted]

1.5.1.4.5 Enterprise Resource Planning (ERP) Application Hosting [C.2.4.2.2.1 (4)]

Application Hosting [Optional]
The contractor (i.e. Application Service Provider [ASP]) shall provide hosted applications including but not limited to: *Enterprise Resource Planning (ERP)* for the management of various functions within a federal Agency, including human resources, finance, procurement, and supply chain

AT&T offers strategic insight, ability to differentiate, increased productivity, and flexibility with a complete Enterprise Resource Planning (ERP) solution. ERP solutions [redacted] **Figure 1.5.1.4-4**. [redacted] an ERP package solution for Agencies that combines everything needed for a fast, proven, and affordable industry solution that enables Government business. [redacted]

[redacted]

Figure 1.5.1.4-4: ERP Cross-Functional Business Processes. *Using mySAP ERP will allow Agencies to develop custom integration and create complete lifecycle management solutions.*

Agencies will receive the [redacted] ERP functionality, including sourcing and manufacturing operations, planning operations, sales and distribution operations, financials, and analytics. The packaged solution implements select ERP functions that support key business processes most critical to the success of Government Agencies and high tech companies. Using it as a foundation, Agencies can take a modular approach to deploy additional functions as needed.

The standard implementation of the [redacted] ERP packaged solution for the high tech industry provides a fast, low-risk path to significant benefits. Agencies can leverage the solution to automate and streamline business processes globally, as well as to easily integrate merged or acquired organizations into core operations.

At the same time, Agencies can leverage the [redacted] platform to rapidly respond to changing market opportunities and make the most of ever-shortening product life cycles by quickly rolling out new applications, integrating other applications, and developing composite applications. The solution also provides increased visibility and control, enabling more timely and effective business decisions across Agency, supplier, and internal operations.

1.5.1.4.6 Human Resource Application Hosting [C.2.4.2.2.1 (4)]

Application Hosting [Optional]
The contractor (i.e. Application Service Provider [ASP]) shall provide hosted applications including but not limited to: *Human Resource Applications* for the administration of benefits, time and labor, salary, pension, et cetera. Moreover, HR systems support self-service applications, allowing managers to initiate personnel actions or change position descriptions, avoiding the burden of paper and e-mails. Employees, using browser-based self-service, can manage life events and benefits, such as health insurance coverage, retirement savings, or changing their W-4.

AT&T will be able to provide Human Resource (HR) applications with leading providers of Human Resources Microsystems (HRMS). AT&T will provide HR management applications, such as payroll, tax processing, and web-based employee self-services.

Agencies can leverage [redacted] to create an integrated HRMS and payroll solution. Agencies can subscribe to [redacted], which provides payroll and payroll tax solutions as described in **Table 1.5.1.4-1**.

SOLUTION	DESCRIPTION
Payment of payroll, through direct deposit and/or paper checks	[redacted]
Automatic preparation and submission of relevant reports and filings	[redacted]
Leverage of existing practices	[redacted]
Real-time access to key information	[redacted]
Access to payroll and payroll tax specialists	[redacted]
Elimination of existing tax jurisdiction headaches	[redacted]

Table 1.5.1.4-1: HRMS Payroll and Payroll Tax Solutions. [redacted]

Supplier agreements with leading providers of [redacted] enable AT&T to provide HR applications to Government Agencies. Partnerships, such as these, can facilitate the implementation of HR management applications such as payroll, tax processing and web-based employee self-services to Government Agencies.

1.5.1.5 Stipulated Deviations

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

1.5.1.6 EMNS Dedicated Hosting (DHS) – Directory Services

The added sections are provided to Agencies ordering Enhanced Managed Network Service (EMNS) and are ordered with other EMNS service components.

1.5.1.6.1 EMNS DHS – Directory Services Description

Enterprise-wide Directory service facilitate the management and utilization of a variety of Information Technology (IT) applications such as file services, network resources, security services, web, e-business, white pages and other object–based services.

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

The Directory Service will conform to the Agency's standards for directory services, and will provide end-users with the ability to interact globally with directory services in a transparent and consistent manner.

1.5.1.7 Value Added EDI Network Hosting

Sterling Commerce, an AT&T company, offers a comprehensive hosted electronic data collaboration solution which provides individual agencies and businesses with advanced data exchange and systems integration, visibility into key business document process management, simplified partner on-boarding and management processes, and end-to-end business process management.

1.5.1.7.1 Service Description

DHS Value Added Network Hosting allows an Agency to subscribe to standard or custom application hosting services. Value Added Network

Hosting provides a shared hosting platform for operating Value Added Network (VAN) applications. The VAN applications are separate from the VAN hosting platform and are available through Application Hosting feature CLINs. [redacted]

The hosted Value Added Network (VAN) managed services provides a complete Business to Business (B2B) solution. [redacted]

The hosting facility has necessary physical and logical security in place as well as the appropriate backup power and heating, ventilation and air conditioning. [redacted]

[redacted]

[redacted] **Figure 1.5.1.7-1** [redacted]

[redacted]

Figure 1.5.1.7-1: [redacted]

1.5.1.7.2 [redacted]

As **Table 1.5.1.7-1** shows, the WAN connectivity from the Agency location to the VAN hosting centers supports [redacted] The VAN service provides communications options via the [redacted] The table below shows the different [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]			[redacted]									

Table 1.5.1.7-1: [redacted]

The Sterling Collaboration Network (SCN) includes an [redacted] Gateway Service, a solution that keeps partners, buyers, sellers and vendors who prefer using the [redacted] protocols connected. [redacted] capable partners who need to exchange documents with [redacted] business partners benefit by relaying their documents through the Sterling Collaboration Network [redacted] This means that Agencies who do not use [redacted] can benefit as they can meet their business partners [redacted] requirements without [redacted]

Sterling Collaboration Network (SCN) interprets and manages the differences in [redacted] By bridging the gap, Agencies can maintain their own EDI strategy – regardless of partner preferences.

Designed to meet the needs of companies of all sizes, the Sterling Collaboration Network [redacted] Gateway:

[redacted]

1.5.1.7.3 Implementation Support

AT&T will provide the necessary implementation support for the VAN service, including the WAN connectivity from the Agency location to the VAN hosting centers. For the WAN connectivity, AT&T can provide any necessary SEDs or the Agency has the option of providing their own Government Furnished Equipment (GFE).

[redacted] **Table 1.5.1.7-2**, [redacted] Based on those options, Agencies have the options of [redacted]

1.5.1.7.4 Provisions

As part of the VAN service, a total "end-to-end" managed solution is provided along with the following provisions:

[redacted]

[redacted]