SUPPLEMENT 2:

State IT Policy, Standard and Service Requirements

Revision History:

Date:	Description of Change:
1/01/2019	Original Version
10/18/2019	Updated to modify service descriptions, include new services, and remove older services. A new Appendix A - Request for Variance to State IT Policy, Standard or Service Requirements was added.

Contents

1. Overview of Supplement

This supplement shall apply to any and all work, services, locations and computing elements that the Contractor will perform, provide, occupy or utilize in conjunction with the delivery of work to the State and any access to State resources in conjunction with delivery of work.

This includes, but is not limited to:

- Major and minor projects, upgrades, updates, fixes, patches and other software and systems inclusive of all State elements or elements under the Contractor's responsibility utilized by the State;
- Any systems development, integration, operations and maintenance activities performed by the Contractor;
- Any authorized change orders, change requests, statements of work, extensions or amendments to this contract;
- Contractor locations, equipment and personnel that access State systems, networks or data directly or indirectly; and
- Any Contractor personnel, or sub-contracted personnel that have access to State Data as defined below:
    - "State Data" includes all data and information created by, created for, or related to the activities of the State and any information from, to, or related to all persons that conduct business or personal activities with the State, including, but not limited to Sensitive Data.
    - "Sensitive Data" is any type of data that presents a high or moderate degree of risk if released, disclosed, modified or deleted without authorization. Sensitive Data includes but is not limited to:
        - Certain types of personally identifiable information (PII) that is also sensitive, such as medical information, social security numbers, and financial account numbers.
        - Federal Tax Information (FTI) under IRS Special Publication 1075.
        - Protected Health Information (PHI) under the Health Insurance Portability and Accountability Act (HIPAA).
        - Criminal Justice Information (CJI) under Federal Bureau of Investigation's Criminal Justice Information Services (CJIS) Security Policy.
    - The data may also be other types of information not associated with an individual such as security and infrastructure records, trade secrets, and business bank account information.
- The terms in this supplement are in addition to the Contract terms and conditions. In the event of a conflict for whatever reason, the highest standard contained in the Contract shall prevail.

Please note that any proposed variances to the requirements outlined in this supplement are required to be identified in Appendix A - Request for Variance to State IT Policy, Standard or Service Requirements. Offerors are asked not to make any changes to the language contained within this supplement. In the event the Offeror finds it necessary to deviate from any of the standards or State IT services, a variance may be requested, and the Offeror must provide a sufficient business justification for the variance request. In the event that a variance is requested post award, e.g., a material change to the architecture, the Enterprise IT Architecture Team will engage with the Contractor and appropriate State stakeholders to review and approve/deny the variance request.

2. State IT Policy and Standard Requirements

The Contractor will comply with State of Ohio IT policies and standards. For the purposes of convenience, a compendium of IT policy and standard links is provided in the table below.

Table 1 – State of Ohio IT Policies, Standards, IT Bulletins and DAS Polices

Item	Link
State of Ohio IT Policies	https://das.ohio.gov/Divisions/Information-Technology/State-of-Ohio-IT-Policies
State of Ohio IT Standards	https://das.ohio.gov/Divisions/Information-Technology/State-of-Ohio-IT-Standards
State of Ohio IT Bulletins	https://das.ohio.gov/Divisions/Information-Technology/State-of-Ohio-IT-Bulletins
DAS Policies	100-11 Protecting Privacy 100-12 ID Badges & Visitors Policy 700-00– Technology / Computer Usage Series 2000-00 – IT Operations and Management Series https://das.ohio.gov/Divisions/Administrative-Support/Employees-Services/DAS-Policies

3. State IT Service Requirements

3.1. Requirements Overview

Contractors performing the work under the Contract are required to comply with the standards and leverage State IT services outlined in this document unless the State has approved a variance. See note above in Section 1 regarding instructions to propose variances to the requirements outlined in this supplement.

3.2. Solution Architecture Requirements

Unless stipulated otherwise in the RFP, on premise or cloud-based solutions are permitted by the State. Custom or unique built solutions must comply with State requirements including using the State's virtualized computing platform (State Private Cloud) or the State of Ohio Enterprise brokered public cloud service and running on databases that comply with the State's supported database platforms. Custom or unique built solutions are required to include installation of third-party applications on State provided computing platforms which could be on the State-run private cloud or the State-run public cloud. Dedicated server platforms are not compliant with the State's virtualization requirements. The State provides different storage pools (tiers) of storage with the ability to use and allocate the appropriate storage type based on predetermined business criticality and requirements. Storage pools are designed to support different I/O workloads. Custom or unique built solutions must take advantage of the State's storage service offerings.

Custom or unique built solutions must be developed in open or industry standard languages (e.g. Java, .NET, PHP, etc.). Applications must be developed with standards-based open application programming interfaces and all available features and functionality accessible via APIs must be disclosed in the proposed solution. Custom or unique built solutions with Open APIs proposed must include periodic updates throughout the project lifecycle and a final update as part of the closure phase.

Cloud-based solutions must utilize as many platform services as possible and comply with State requirements to run in the State of Ohio Enterprise brokered public cloud service. Currently, Microsoft Azure and Amazon Web Services are hosted by DAS OIT for the State of Ohio.

3.3. State of Ohio IT Services

The Department of Administrative Services Office of Information Technology (DAS OIT) delivers information technology (IT) and telecommunication services. DAS OIT is responsible for operating and maintaining IT and telecommunication hardware devices, as well as the related software. This document outlines a range of service offerings from DAS OIT that enhance performance capacity and improve operational efficiency. Explanations of each service are provided and are grouped according to the following solution categories.

1. InnovateOhio Platform

Executive Order 2019-15D, "Modernizing Information Technology Systems in State Agencies," established the InnovateOhio Platform (IOP) initiative. IOP focuses on digital identity, the experience of the individual authorized to access the system ("User"), analytics and data sharing capabilities. The InnovateOhio Platform provides integrated and scalable capabilities that better serve Ohioans.

Digital Identity Products

OH | ID - Digital identity solution for Ohio citizens:

Provides single sign-on for disparate systems, enhanced security and privacy, federal and state compliance, and personalized experience. Simple, secure access for citizens. Multiple levels of identity assurance.

- Single Sign-On
- Access Logging
- Real-Time Analytics
- 2-Factor Authentication (2FA)
- Access Management
- Self-Service Portal
- Identity Proofing
- Directory Integration

OH | ID Workforce - Digital identity solution for Ohio workforce

Provides single sign-on for disparate systems, enhanced security and privacy, federal and state compliance, and personalized experience. Simple, secure access for state and county employees, contractors, and external workers. Multiple levels of identity assurance.

- Single Sign-On
- Directory Integration
- Real-Time Analytics
- 2-Factor Authentication (2FA)
- Just-in-Time Provisioning
- User Management
- Access Logging
- Privileged Access Management

ID Platform – Software as a Service (SaaS) identity framework

Provides an authorization layer and allows for the integration and extension of InnovateOhio Platform identity services into applications. Customizable to User needs.

- Fine-Grain Authorization Management
- Real-Time Analytics
- Extendable Services from OH|ID
- Cloud-Based Infrastructure

User Experience Products

IOP Portal Builder - Website template accelerator:

An accelerator to easily create modern, responsive and ADA-compliant websites and portals for the InnovateOhio cloud platform. The InnovateOhio Portal Builder is available in a Software as a Service (SaaS) form.

- Standardized Dynamic Templates
- Automated Workflows
- Governance & Access Control
- Optimized Content Search
- ADA-Compliant
- Content Management
- Integration with OH|ID
- Real-Time Analytics
- Aggregate Applications
- Customizable Features
- Mobile Ready
- Site Analytics

IOP myOhio - The State's Intranet platform

Features intuitive navigation, simplified access to on-boarded business applications, and a modernized, mobile-responsive design. Automates compliance with accessibility standards per Section 508 of the Rehabilitation Act.

- Single Sign-On
- Personalized Content
- Content Management
- Near Real-Time Syndication
- 2-Factor Authentication (2FA)
- Access Logging
- Optimized Content Search
- Application Store
- Mobile Ready
- Automated Workflows
- Real-Time Analytics
- Site Analytics

IOP Digital Toolkit - Free User experience digital toolkit

Reusable components for quick deployment of websites, portals and applications. Universal framework for developers and designers. Consistent and compliant User experiences.

- Mobile Ready
- Real-Time Analytics
- Style Guide
- Customizable Features
- Sample Code
- ADA-Compliant
- Standardized Dynamic Templates

Analytics and Data Sharing Products

Applied Analytics

Ohio's applied analytics solution provides the ability to build analytical and reporting solutions and deploy them in the most impactful manner possible by putting data in the hands of Users in their natural workflow. From ideation and solution design to data science and engineering, the applied analytics solution enables the User to move from concept to results.

- Advanced Data Science
- Data Strategy Optimization
- Ideation & Scoping
- Solution Design
- Visual Data Discovery
- Workflow Integration

Big Data Platform

Ohio's data sharing and analytics platform provides public/private cloud deployment models that are secure, flexible, and scalable, powering analytics across data of any type or source to gain deeper insights and drive impactful outcomes.

- Data Sharing
- Diverse Data
- Hybrid Cloud
- Massive Volumes
- Rapid Prototyping
- Real-Time Analytics
- Security & Compliance

Data Management

Ohio's self-service data management suite provides rich and secure capabilities to harness the power of the analytics platform leveraging User friendly and pre-configured technologies. Additionally, the suite supports a bring-your-own-tool approach allowing analysts and data scientists to work on the platform with the technologies they are most comfortable using.

- Audit
- Bring Your Own Tool (BYOT)
- Data Engineering
- Data Exploration
- Data Lineage
- Data Profiling
- Governance & Security
- Pre-Built Pipelines
- Self-Service Support

Please explain how the InnovateOhio Platform will be incorporated into the proposed solution. If this section, or portions of this section, are not applicable, please explain and note as N/A. Please note that any proposed variances must be noted in Appendix A – Request for Variance to State IT Policy, Standard or Service Requirements. The language within the supplement shall not be modified.

GTL Response: Not applicable.

To maximize the security of our networks, and maximize performance of the supplied systems, we recommend the applications go through a separate, dedicated network provided and maintained by GTL. We recognize some interfaces to your IT infrastructure are required (e.g. integration to JMS and commissary systems).

Should elements of ODRC's IT infrastructure (e.g. customer wireless access points) need to be used, GTL recommends VLAN segmentation and firewall deployment to control the information allowed between networks. We will work with your IT personnel to implement such an arrangement. Note however, we do not recommend the combination of GTL system and ODRC networks as, in our experience, this configuration has caused issues when not occurring within a dedicated network.

GTL services to incarcerated individuals are accessible only through GTL-provided hardware and through GTL's private, secure network. Management tools for ODRC authorized staff are web-based. Tools accessible to the friends and family of ODRC's incarcerated individuals are web-based or available through GTL's mobile apps.

2. Application Services

Enterprise Document Management Solution (DMS):

The Enterprise Document Management Solution (DMS) is a standardized, integrated solution for document and content management. The core components of the solution include:

- **Document Management** core capabilities such as: secure check-in / check-out, version control, and index services for business documents, audio / video files, and Environmental Systems Research Institute (ESRI) / Geographic Information Systems (GIS) maps.
- **Image Processing** for capturing, transforming and managing images of paper documents via scanning and / or intelligent character recognition technologies such as Optical Character Recognition.
- **Workflow / Business Process Management (BPM)** for supporting business processes, routing content, assigning work tasks and creating audit trails.
- **Records Management** for long-term retention of content through automation and policy, ensuring legal, regulatory and industry compliance.
- **Web Content Management (WCM)** for controlling content including content creation functions, such as templating, workflow and change management and content deployment functions that deliver content to Web servers.
- **Extended Components** can include one or more of the following: Digital Asset Management (DAM), Document Composition, eForms, search, content and analytics, e-mail and information archiving.

Electronic Data Interchange (EDI) Application Integration:

EDI Application Integration service is a combination of Application Integration, Data Exchange and Electronic Data Interchange (EDI) functionality. This service provides application to application connectivity to support interoperable communication, data transformation, and business process orchestration amongst applications on the same or different computing platforms. Business process orchestration between many data formats may be supported including Web Services, XML, People-Soft, FTP, HTTP, MSMQ, SQL, Oracle, Flat File, SAP, DB2, CICS, EDI, HIPAA, HL7, Rosetta Net, etc.

The Data Exchange component allows unattended delivery of any electronic data format via encrypted files over public FTP, FTPS, SFTP, VPN. Application Integration services are offered via:

- **End Points** – also referred to as a mailbox, this is a connectivity point to facilitate the movement or transaction of data between two or more entities.
- **KBs** – represents the size in kilobytes of a message that is transformed or processed. This typically refers to a document or file conversion or a format change.
- **Messages** – a discrete unit of data that is moved or transacted between two or more entities. A message typically represents a business document or a file.

Enterprise Business Intelligence (BI):

The State of Ohio Enterprise Business Intelligence (BI) service provides enterprise data warehousing, business and predictive analytics, and decision support solutions. By turning raw data into usable information, BI helps Users analyze policies and programs, evaluate operations, and drive decisions. The core information available for analysis includes:

Health and Human Services Information

- Ohio Benefits
- Medicaid Claims
- Medicaid Enrollment
- Medicaid Financial
- Medicaid Provider

- Long Term Care
- Medicare Claims
- Pharmacy

Financial Information

- General Ledger
- Travel and Expense
- Procure to Pay
- Capital Improvements
- Accounts Receivable
- Asset Management
- Budget/Planning
- Value Management
- Statewide Cost Allocation Plan
- Minority Business Enterprise (MBE) Program/Encouraging Diversity, Growth and Equity (EDGE) Program

Workforce and Human Resources

- Workforce Profile
- Compensation
- State of Ohio Payroll Projection Systems
- ePerformance
- Enterprise Learning Management

Enterprise eLicense:

Enterprise eLicense is the State of Ohio's online system used to manage the issuance, certifications, inspections, renewals and administration of professional licenses across the State. The eLicense application is a public/business facing system that is designed to foster the creation and growth of businesses in the State. The system is a central repository for license and certificate data, in addition to managing the generation and storage of correspondence. Secure fee collection is performed through an on-line payment processor, which includes bank transfers, credit cards, and other payment types. Core system capabilities include:

Customer Relationship Manager (CRM)

- Contact Management

Revenue

- Deposit Accounting Revenue Tracking
- Refund and Reimbursement Processing
- Fine and Penalty Tracking

License Administration

- Administration
- Workflow
- Reports

Enforcement

- Enforcement Activities
- Case Management Activities

Online Licensure Services

- Applications
- Renewals
- License Verification
- License Maintenance
- License Lookup Website
- Workflow
- Document Management
- Secure Payment Processing

Other Services

- Continuing Education Tracking
- Examinations

- Inspections
- Complaint Management

ePayment Business Solution:

The CBOSS ePayment Gateway solution is a highly flexible payment engine supporting a wide range of payment types: credit cards, debit cards, electronic checks, as well as recurring, remote capture and cash payments. The CBOSS ePayment Gateway solution utilizes a single, common gateway to permit the acceptance of payments from multiple client application sources: Web, IVR, kiosk, POS, mobile, over the counter, etc. Payment processing is supported through multiple credit card gateway options, automated clearing house (ACH) bank processing, and Telecheck services.

The CBOSS ePayment Gateway solution is compliant with the Payment Card Industry Data Security Standard (PCI DSS), the Electronic Fund Transfer Act (EFTA) and is audited to the standards of SSAE16 SOC1 Type II.

Enterprise eSignature Service:

OneSpan Sign is Ohio's enterprise solution for eSignatures. The product is a FedRAMP SaaS (Software as a Service) solution, which offers a standardized approach to cloud security. OneSpan Sign's eSignature functions include workflows, tracking, audit logs and protection against forgery/non-repudiation.

OneSpan Sign has an extensive library of open application programming interfaces (APIs) to integrate eSignatures with existing applications and core systems. OneSpan Sign's pre-built, third-party connectors enable the eSignature capabilities into business software products such as Dynamics CRM, Salesforce, Microsoft SharePoint, etc.

IT Service Management Tool (ServiceNow):

DAS OIT offers ServiceNow, a cloud-based IT Service Management Tool that provides internal and external support through an automated service desk workflow-based application which provides flexibility and ease-of-use. ServiceNow provides workflows aligning with Information Technology Infrastructure Library (ITIL) processes such as incident management, request fulfillment, problem management, change management and service catalog. These processes allow for the management of related fields, approvals, escalations, notifications and reporting needs.

Standard ServiceNowFeatures Include:

- **Incident Management** - Manage service disruptions and restore normal operation quickly.
- **Problem Management** - Identify the underlying cause of recurring incidents.
- **Change Management** - Minimize the impact of service maintenance.
- **Configuration Management** - Define and maintain a configuration management database (CMDB) for IT infrastructure.
- **Asset Management** - Manage assets and inventory records.
- **Service Catalog Management** – Automated process for goods and service requests.
- **Knowledge Management** - Gather, store and share knowledge within the organization.
- **Reporting** – Custom reporting.
- **Integration to AD, Event Monitoring, Discovery Tools, Exchange** – Integration to AD, Event Monitoring, Discovery Tools, Exchange – Integration with third-party applications.
- **Customized Portal Pages** – User friendly interface to create engaging and robust portals, dashboards, and applications.
- **Software Asset Management** – End to end software life cycle management on a single platform, to optimize spend and reduce compliance risk.
- **IT Operations Management (ITOM)** - Includes event management, service mapping, discovery, orchestration and cloud management.

Ohio Benefits:

Ohio Benefits provides a comprehensive and effective platform for planning, designing, development, deployment, hosting and ongoing maintenance of all State of Ohio Health and Human Services (HHS) Public Assistance Services and Programs.

Ohio Benefits provides superior eligibility services including citizen self-service, efficient workflow management and coordination, an agile and easily manageable rules engine, improved data quality and decision support capabilities. Ohio Benefits supports improvement in State and county productivity, capability and accessibility of benefits to Ohioans through a robust enterprise system. The Ohio Benefits platform provides four distinct technology domains:

1. **Common Enterprise Portal** – User Interface and User Experience Management, Access Control, Collaboration, Communications and Document Search capability.
2. **Enterprise Information Exchange** – Discovery Services (Application and Data Integration, Master Data Management (MDM), Master Person Index and Record Locator Service), Business Process Management, Consent Management, Master Provider Index and Security Management.
3. **Analytics and Business Intelligence** – Integration and delivery of analytics in the form of alerts, notifications and reports.
4. **Integrated Eligibility** – A common Enterprise Application framework and Rules Engine to determine eligibility and benefits for Ohio Public Benefit Programs.

Privacy and security are the foundational blocks of the platform which is compliant with all State and federal standards.

Ohio Business Gateway (OBG):

The Ohio Business Gateway (OBG) offers Ohio's businesses a time and money saving online filing and payment system that simplifies business' relationships with government. Ohio businesses can use OBG to access various services and electronically submit transactions and payments. The OBG also offers the ability for business to view historical filings (and payments) and allows for business activities to be provided by a third-party provider of professional accounting services. OBG Electronic Filing also partners with local governments to enable businesses to file and pay selected Ohio municipal income taxes.

OBG Electronic Filing routes data and payment information directly to program administrators so that they may continue to manage the overall account relationship.

Ohio Administrative Knowledge System (OAKS):

The Ohio Administrative Knowledge System (OAKS) is the State's Enterprise Resource Planning (ERP) system which provides central administrative business services such as Financial Management, Human Capital Management, Content Management, Enterprise Learning Management and Customer Relationship Management. Core system capabilities include:

Content Management (myohio.gov)

- Centralized Communications to State Employees and State Contractors
- OAKS alerts, job aids and news
- Statewide News
- Password Reset for Active Directory

Customer Relationship Management (CRM)

- Contact / Call Center Management

Enterprise Business Intelligence

- Key Financial and Human Resources Data, Trends and Analysis
- Cognos driven reporting
- Targeted Business Intelligence
- Tableau Analytics and Visualization

Enterprise Learning Management (ELM)

- Training Curriculum Development
- Training Content Delivery
- Training Status Tracking and Reporting

Financial Management (FIN)

- Accounts Payable
- Accounts Receivable
- Asset Management
- Billing
- eSourcing
- Financial Reporting
- General Ledger
- Planning and Budgeting
- Procurement

- Travel & Expense

Human Capital Management (HCM)

- Benefits Administration
- eBenefits
- ePerformance
- Kronos
- Payroll
- Position Management
- Time and Labor
- Workforce Administration

Enterprise Geocoding Services (EGS):

Enterprise Geocoding Services (EGS) combine address standardization, geocoding, and spatial analysis into a single service. Individual addresses can be processed in real time for online applications or large numbers of addresses can be processed in batch mode.

Geographic Information Systems (GIS) Hosting:

GIS Hosting delivers dynamic maps, spatial content, and spatial analysis via the Internet. Users can integrate enterprise-level GIS with map capabilities and spatial content into new or existing websites and applications.

Please explain how the State's Application Services will be incorporated into the proposed solution. If this section, or portions of this section, are not applicable, please explain and note as N/A. Please note that any proposed variances must be noted in Appendix A – Request for Variance to State IT Policy, Standard or Service Requirements. The language within the supplement shall not be modified.

GTL Response: Not applicable.

To maximize the security of our networks, and maximize performance of the supplied systems, we recommend the applications go through a separate, dedicated network provided and maintained by GTL. We recognize some interfaces to your IT infrastructure are required (e.g. integration to JMS and commissary systems).

Should elements of ODRC's IT infrastructure (e.g. customer wireless access points) need to be used, GTL recommends VLAN segmentation and firewall deployment to control the information allowed between networks. We will work with your IT personnel to implement such an arrangement. Note however, we do not recommend the combination of GTL system and ODRC networks as, in our experience, this configuration has caused issues when not occurring within a dedicated network.

3. Data Center Services

Advanced Interactive eXecutive (AIX):

AIX is a proprietary version of the UNIX operating system developed by IBM. DAS OIT runs the AIX operating system on IBM Power hardware, as a physical server or logical partition (LPAR)/virtual server. All of the AIX systems are connected to the DAS OIT Enterprise Storage Area Network (SAN) for performance, general purpose or capacity-based storage. All systems are also provided backup and recovery services.

Backup:

The Backup service uses IBM Tivoli Storage Manager Software and provides for nightly backups of data. It also provides for necessary restores due to data loss or corruption. The option of performing additional backups, archiving, restoring or retrieving functions is available. DAS OIT backup facilities provide a high degree of stability and recoverability as backups are duplicated to the alternate site.

Data Center Co-Location:

The DAS OIT Co-Location service offers a Tier 3 capable secure data center environment with reliable uptime, power redundancy and redundant cooling to ensure uninterrupted access of critical data and applications in the State of Ohio Computer Center (SOCC). The SOCC is staffed and available to authorized personnel 24x7x365 and is accessible via electronic card key only.

Data Storage:

The services covered under Data Storage include:

High Performance Disk Storage service offers high-performance, high-capacity, secure storage designed to deliver the highest levels of performance, flexibility, scalability and resiliency. The service has fully redundant storage subsystems, with greater than five-nines availability, supporting mission critical, externally-facing and revenue-generating applications 24x7x365. High Performance Disk Storage is supplied as dual Enterprise SAN fiber attached block storage.

General Purpose Disk Storage service offers a lower-cost storage subsystem, which is not on a high performance disk. This service supports a wide range of applications, including email, databases and file systems. General Purpose Disk is also flexible and scalable and highly available. General Purpose Disk Storage is supplied as dual Enterprise SAN fiber attached block storage.

Capacity Disk Storage service is the least expensive level of disk storage available from DAS OIT. Capacity Disk is suitable for large capacity, low performance data, such as test, development and archival. Capacity Disk Storage is supplied as dual Enterprise SAN fiber attached block storage or as file-based storage.

Distributed Systems DRaaS:

Distributed Systems Disaster Recovery as a Service (DRaaS) offers server imaging and storage at a geographically disparate site from Columbus. The service provides a private Disaster Recovery as a Service solution connected to the State of Ohio Computer Center (SOCC) via the Ohio One Network that will consists of the following:

- Compute to allow expected performance in the event of a complete failover
- 24vCPU per host with 32 host in the environment all licensed with VMWare
- Support of the orchestration and replication environment
- Site connectivity
- Stored images available upon demand

Open Systems Disaster Recovery - Windows (1330 / 100607 / DAS505170/ 3854L) - Open Systems Disaster Recovery – Windows is a service that provides a secondary failover site for Windows based servers within the geographically disparate site. This service provides duplicative server compute and storage to match Server Virtualization and Data Storage capabilities as provisioned at the SOCC. This service is provided through a contracted third party who is responsible for all management and equipment at the facility.

Open Systems Disaster Recovery - AIX (1330 / 100607 / DAS505170/ 3854N) - Open Systems Disaster Recovery – AIX is a service that provides a secondary failover site for AIX based servers within the geographically disparate site. This service provides duplicative server compute and storage to match AIX Systems Services and Data Storage capabilities as provisioned at the SOCC. This service is provided through a contracted third party who is responsible for all management and equipment at the facility.

Mainframe Business Continuity and Disaster Recovery:

Business continuity involves planning for keeping all aspects of a business functioning in the midst of disruptive events. Disaster recovery, a subset of business continuity focuses on restoring the information technology systems that support the business functions.

Mainframe Disaster Recovery (DR) services are available for DAS OIT's IBM mainframe environment. Services are made available via IBM's Business Continuity and Resiliency Services, which provides hot site computer facilities at a remote location.

Tests are conducted bi-annually at IBM's hot site location, during which DAS OIT's mainframe computer infrastructure is restored. Once the mainframe system is operational, production applications are restored and extensive tests are conducted to ensure that those applications have been successfully recovered and would be available in the event of an actual disaster.

This service is designed to expand business continuity and disaster recovery capabilities in the most cost effective and efficient manner possible.

Mainframe Systems:

DAS OIT's Mainframe Systems services offer an IBM mainframe computer sysplex with a processing speed rating at 5,700 Million of Instructions per Second (MIPS). This mainframe uses the z/OS operating system and the Job Entry Subsystem (JES3). Additionally, the system is connected via fiber to DAS OIT's High Performance Disk Storage, which affords reliable and fast disk access and additional storage capacity when needed.

Services are provided using a wide range of application, transaction processing and telecommunications software. Data security and User authentication are provided by security software packages. Mainframe tape service option is available:

- Mainframe Virtual Tape - Virtual tape technology that optimizes batch processing and allows for better tape utilization using the EMC Disk Library for Mainframe (DLM) virtual tape.

Metro Site Facility:

The Metro Site Facility Service provides a secondary, near real-time (measured in ms) failover from the SOCC. This service provides for the facility, site connectivity, on-going support of server images for Disaster Recovery as a Service, and associated services. Metro Site Facilities are for the support of Virtual Server and Data Storage, providing Global/Metro Mirroring at a secondary near real time failover site within the Metro Columbus area.

Server Virtualization:

Server Virtualization is the practice of abstracting the physical hardware resources of compute, storage and networking of a host server and presenting those resources individually to multiple guest virtual servers contained in separate virtual environments. DAS OIT leverages the VMware vSphere platform to transform standardized hardware into this shared resource model that is capable providing solutions around availability, security and automation.
Server Virtualization includes:

- **DAS OIT Managed Basic Server Virtualization:** DAS OIT hosts the virtual server and manages the hardware/virtualization layer. DAS OIT is also responsible for managing the server's operating system (OS). This service includes 1 virtual CPU (vCPU), 1 GB of RAM and 50 GB of General Disk Storage used for the operating system.

Please explain how the State's Data Center Services will be incorporated into the proposed solution. If this section, or portions of this section, are not applicable, please explain and note as N/A. Please note that any proposed variances must be noted in Appendix A – Request for Variance to State IT Policy, Standard or Service Requirements. The language within the supplement shall not be modified.

GTL Response: Not applicable.

To maximize the security of our networks, and maximize performance of the supplied systems, we recommend the applications go through a separate, dedicated network provided and maintained by GTL. We recognize some interfaces to your IT infrastructure are required (e.g. integration to JMS and commissary systems).

Should elements of ODRC's IT infrastructure (e.g. customer wireless access points) need to be used, GTL recommends VLAN segmentation and firewall deployment to control the information allowed between networks. We will work with your IT personnel to implement such an arrangement. Note however, we do not recommend the combination of GTL system and ODRC networks as, in our experience, this configuration has caused issues when not occurring within a dedicated network.

4. Hosted Services

Database as a Service:

Database as a Service provides an enterprise database solution that is easy to use and simple to update without incurring the cost of setting up and maintaining an enterprise database environment through which scaling, load balancing, failover and backup can all be managed. DAS OIT Database Specialists ensure that all aspects of handling data are taken care of which includes, but is not limited to, storage, backups, tuning and security.

Current Database Solutions being offered:

- SQL Server
- Oracle
- DB2

Oracle Exadata DBaaS:

- **Starter/Small Database:** 2 Cores, 6GB Ram, 200GB min Storage, *Up to 2 databases
  Entry level database environment for small applications.
- **Medium Database:** 4 Cores, 8 GB Ram, 500GB Min Storage, *Up to 4 databases
  Medium sized database environment for DB consolidation.
- **Large Database:** 6 Cores, 12GB Ram, 1TB Min Storage, *Up to 6 Databases
  Optimal service for large, complex database and data warehouse environments.

*The maximum number of databases is dependent upon the database size and actual usage.

Based on the model the proposed service model for DAS OIT includes the following structure:

- **Small**: 2 Core = 1 billable unit per month.
- **Medium**: 4 Cores = 2 billable units per month.
- **Large**: 6 Cores = 3 billable units per month.

Database Support:

Database Support provides technical assistance for database implementation and usage. Services utilized may include any or all of the following service offerings: installation, upgrade and management of database software, database administration tools and packaged application database products, backup/recovery procedure implementation, monitoring, tuning and troubleshooting.

Please explain how the State's Hosted Services will be incorporated into the proposed solution. If this section, or portions of this section, are not applicable, please explain and note as N/A. Please note that any proposed variances must be noted in Appendix A – Request for Variance to State IT Policy, Standard or Service Requirements. The language within the supplement shall not be modified.

GTL Response: Not applicable.

To maximize the security of our networks, and maximize performance of the supplied systems, we recommend the applications go through a separate, dedicated network provided and maintained by GTL. We recognize some interfaces to your IT infrastructure are required (e.g. integration to JMS and commissary systems).

Should elements of ODRC's IT infrastructure (e.g. customer wireless access points) need to be used, GTL recommends VLAN segmentation and firewall deployment to control the information allowed between networks. We will work with your IT personnel to implement such an arrangement. Note however, we do not recommend the combination of GTL system and ODRC networks as, in our experience, this configuration has caused issues when not occurring within a dedicated network.

Inmate Telephone System

GTL's ITS is a centralized non-premise system configured with built-in redundancy to reduce service interruption and prevent data loss. All call and system data are stored at GTL Data Centers with integrated redundancy. Transmission of data to off-site databases and servers at our facilities are encrypted according to IPsec protocols.

ITS system data for ODRC will be stored in our secure, scalable, high availability enterprise class All Flash data storage with encryption at our Primary Data Center. The data for is automatically replicated to an enterprise class NAS storage server.

The GTL platform operates automatically in a **dynamic, real-time environment**. Call records are created and saved with encryption to the All Flash storage in the Primary Data Center. A redundant copy of the call record is automatically replicated to All Flash storage located in the GTL Secondary Data Center. When the call is finished, an exact copy of the completed call record (minus the recording) is transmitted to GTL's Call Control Center.

5. IT Security Services

Secure Sockets Layer (SSL) Digital Certificate Provisioning:

SSL Digital Certificate Provisioning service provides SSL Certificate service across multiple enterprise service offerings. SSL certificates are used to provide communication security to various web sites and communications protocols over the internet (ex. Web Servers, Network Devices, Application Servers, Internet Information Server (IIS), Apache, F5 devices and Exchange servers). SSL Digital Certificate Provisioning supports the delegation of administration and reporting processes while leveraging a common portal.

In addition, please review the Security Supplement (Supplement S - State Information Security and Privacy Requirements and State Data Handling Requirements).

Please explain how the State's IT Security Services will be incorporated into the proposed solution. If this section, or portions of this section, are not applicable, please explain and note as N/A. Please note that any proposed variances must be noted in Appendix A – Request for Variance to State IT Policy, Standard or Service Requirements. The language within the supplement shall not be modified.

GTL Response:

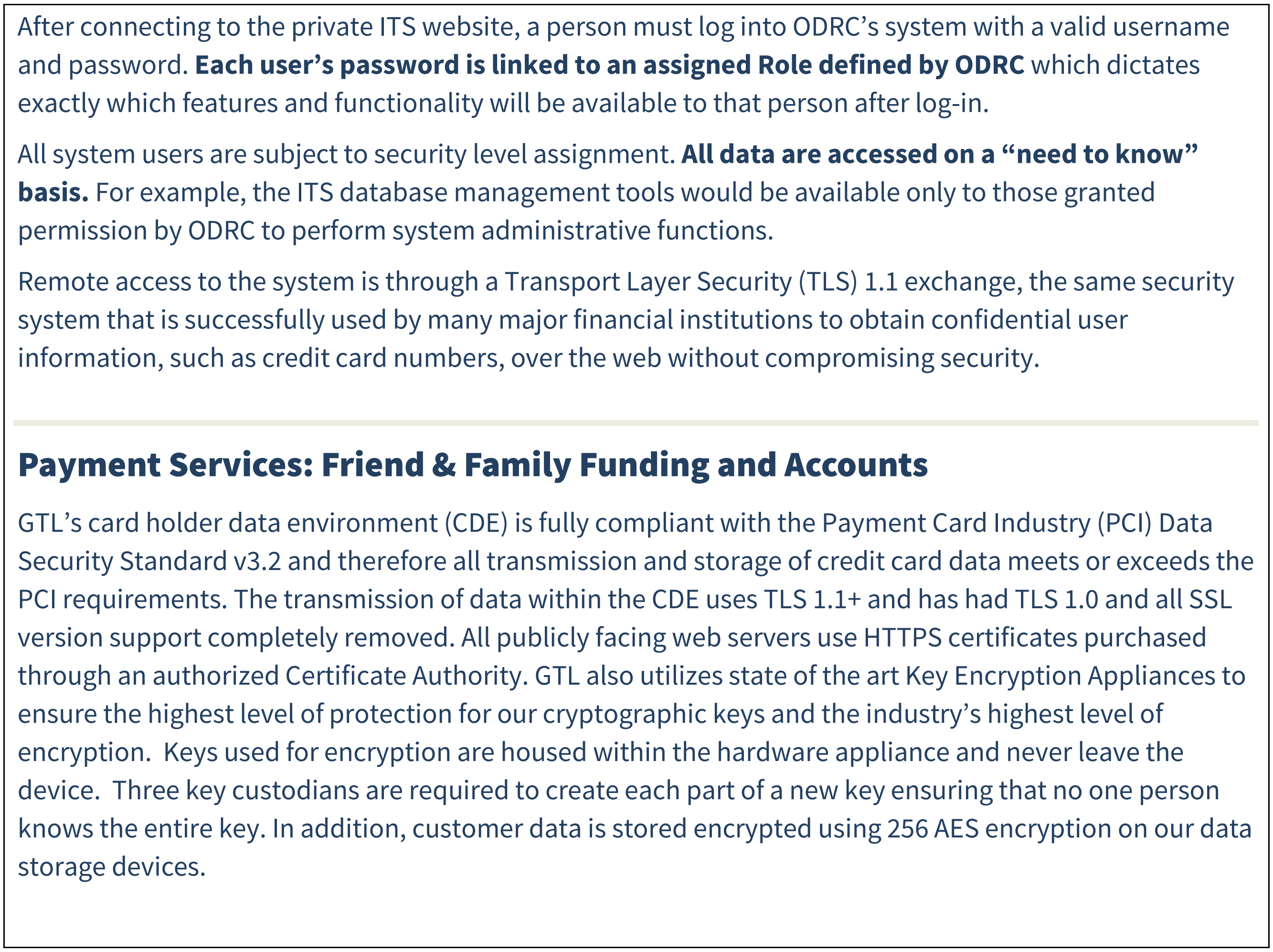
GTL understands that our corrections clients demand the highest levels of data security both for user access of data and storage of that data. At GTL we are dedicated to the protection and reliability of our customers' data using the latest technology and industry best practices. It is the peace of mind that comes with knowing GTL can meet or exceed the data security needs of our clients.

Facility management tools for GTL's services are internet-facing. All data is encrypted during transport using TLS for all customer data in transit over the internet. GTL utilizes TLS 1.1 and higher.

Anytime, Anywhere Access

GTL's hosted Inmate Telephone System (ITS) solution has a Web-based interface that is accessible to authorized individuals via connection to GTL's private ITS website.

The GTL ITS provides Anywhere Anytime Access to its powerful, technologically advanced features. Properly authorized users may access the system from an onsite system workstation, ODRC's on-site PCs, or any off-site PC (desktop or laptop). Compatible smart phones with Internet connection can also access certain ITS features.


After connecting to the private ITS website, a person must log into ODRC's system with a valid username and password. **Each user's password is linked to an assigned Role defined by ODRC** which dictates exactly which features and functionality will be available to that person after log-in.

All system users are subject to security level assignment. **All data are accessed on a "need to know" basis.** For example, the ITS database management tools would be available only to those granted permission by ODRC to perform system administrative functions.

Remote access to the system is through a Transport Layer Security (TLS) 1.1 exchange, the same security system that is successfully used by many major financial institutions to obtain confidential user information, such as credit card numbers, over the web without compromising security.

Payment Services: Friend & Family Funding and Accounts

GTL's card holder data environment (CDE) is fully compliant with the Payment Card Industry (PCI) Data Security Standard v3.2 and therefore all transmission and storage of credit card data meets or exceeds the PCI requirements. The transmission of data within the CDE uses TLS 1.1+ and has had TLS 1.0 and all SSL version support completely removed. All publicly facing web servers use HTTPS certificates purchased through an authorized Certificate Authority. GTL also utilizes state of the art Key Encryption Appliances to ensure the highest level of protection for our cryptographic keys and the industry's highest level of encryption. Keys used for encryption are housed within the hardware appliance and never leave the device. Three key custodians are required to create each part of a new key ensuring that no one person knows the entire key. In addition, customer data is stored encrypted using 256 AES encryption on our data storage devices.

6. IT Support Services

Enterprise End User Support:

Enterprise End User Support is a standardized, fully managed endpoint computing service. This Service uses enterprise tools and standards. This comprehensive service includes e-mail, network connectivity, device procurement, printer support, security policy maintenance, system monitoring, software updates and patching, software deployment to individuals and devices and inventory software and hardware. IT assets provided with the Enterprise End User Support include:

- Dedicated on-site technician
- Break/Fix
- Enterprise Image
- System Center Configuration Management (SCCM)
- Patch Management through SCCM
- Application packaging and deployment
- Asset management (hardware)
- Asset management (software)
- Application usage report provided upon request

Enterprise Virtual Desktop:

Enterprise Virtual Desktop service takes advantage of the Enterprise Private Cloud to store all electronic data via a virtual desktop. The service provides a platform with access to Microsoft Windows and State of Ohio business applications from any device, from any location, at any time.
The Enterprise Virtual Desktop service offers the following:

- **Hosted** - The unmanaged service provides an isolated and dedicated environment that is managed by DAS OIT. This hosted service includes a provisioning portal, a basic window image and a basic group policy for desktops but does not include management or deployment of specific software or desktop provisioning.

- **Managed** - The managed service provides an isolated and dedicated environment that is managed by DAS OIT including desktops and software deployment. The Managed service also includes all Hosted services, software packaging and updating, management of the operating system, deployments and updates.

Please explain how the State's IT Support Services will be incorporated into the proposed solution. If this section, or portions of this section, are not applicable, please explain and note as N/A. Please note that any proposed variances must be noted in Appendix A – Request for Variance to State IT Policy, Standard or Service Requirements. The language within the supplement shall not be modified.

GTL Response: Not applicable.

Authorized users of GTL's system management interface can access online integrated help information as well as take advantage of 24/7 technical support services.

ODRC can expect the finest level of technical support and the very best customer service for the families and friends of inmates who use GTL services. Technical support and billing services are provided entirely without cost to ODRC.

Emphasis on Customer Service

Our comprehensive, trustworthy approach to service is outlined below.

- **Technical Support:** 24 hours a day, 365 days a year, requests for service or reports of malfunctions go directly to GTL's Technical Service Center. Highly trained GTL professionals then determine the best course of action. Our toll-free technical service number is always answered by a live GTL representative.
- **Local Maintenance and Repair**: Field service technicians provided by, and certified by, GTL perform on-site repairs and routine maintenance for our installed systems. They are always available to respond to emergencies
- **Customer Call Center**: GTL provides relatives and friends of inmates with toll-free access to our knowledgeable customer call center staff seven days a week, 24 hours a day. We provide live customer service in both English and Spanish.
- **Proactive System Monitoring:** Systems installed by GTL are continuously monitored by experts in GTL's network and technical centers. Our network monitoring tools and system self-diagnostic features alert GTL to outages or major malfunctions, allowing us to quickly mobilize resources to address the problem. Changes in system performance, above or below defined thresholds, generate automatic alerts that allow us to proactively intervene before a minor issue progresses to the point of disrupting service.

7. Messaging Services

Microsoft License Administration (Office 365):

The Office 365 service provides the ability to use email, Office 365 ProPlus, instant messaging, online meetings and web conferencing, and file storage all from the Cloud, allowing access to services virtually anytime and from anywhere and includes email archiving and eDiscovery services.

The Office 365 service provides licensing and support for email, Office 365 ProPlus (Outlook, Word, Excel, PowerPoint, Publisher, Skype for Business and OneNote), SharePoint, and OneDrive for Business. Microsoft Office Suite includes:

- Email in the Microsoft Cloud

- Office 365 ProPlus
- Skype for Business
- SharePoint Online
- OneDrive for Business

Please explain how the State's Messaging Services will be incorporated into the proposed solution. If this section, or portions of this section, are not applicable, please explain and note as N/A. Please note that any proposed variances must be noted in Appendix A – Request for Variance to State IT Policy, Standard or Service Requirements. The language within the supplement shall not be modified.

GTL Response: Not applicable.

GTL is not providing inter-personnel communication services.

8. Network Services

Offeror's solutions must work within the State's LAN / WAN infrastructure.

Ohio One Network:

The State of Ohio's One Network is a unified solution that brings together design, engineering, operations, service delivery, security, mobility, management, and network infrastructure to target and solve key government challenges by focusing on processes, procedures, consistency and accountability across all aspects of State, city and local government.

Ohio One Network can deliver an enterprise network access experience regardless of location or device and deliver a consistent, reliable network access method.

Secure Authentication:

The DAS OIT Secure Authentication service provides a managed two-factor User authentication solution. The authentication function requires the User to identify themselves with two unique factors, something they know and something they have, before they are granted access. Whether local or remote, this service ensures that only authorized individuals are permitted access to an environment.

Wireless as a Service:

Wireless as a Service is the IT Enterprise Wireless hosted network. This service is an all-inclusive enterprise level wireless LAN solution that offers guest, employee, voice and location-based services with 24/7 target availability.

Coverage is three tiered:

- Broad coverage – small number of Users with low throughput, i.e. public hot spot, warehouse.
- General data use – most common, general computing with robust data performance.
- High capacity use (Voice) – maximum capacity, high bandwidth Users, i.e. location and tracking service.

Please explain how the State's Network Services will be incorporated into the proposed solution. If this section, or portions of this section, are not applicable, please explain and note as N/A. Please note that any proposed variances must be noted in Appendix A – Request for Variance to State IT Policy, Standard or Service Requirements. The language within the supplement shall not be modified.

GTL Response: Not applicable.

GTL provides WAN connectivity to facilities. All sites are protected by a stateful packet inspection firewall. In addition, access control lists (ACLs) limit all inbound and outbound traffic to GTL specific networks which include the IP address for GTL Data Centers, GTL web applications, and ODRC specific network IP address.

GTL creates a virtual private network to all facilities using Internet Protocol Virtual Private Network (IPVPN) technology. All sites are connected to GTL Data Centers using 128-bit AES or 3DES encrypted data links. All validation, call records, and recordings are thus encrypted when they traverse this network. Facilities with remote workstations or cellular wireless broadband networks also use IPVPN and are protected by a firewall.

Already installed and operating at ODRC, the GTL network is handled and maintained entirely by GTL. There is no interaction with the ODRC's network and rarely a need to open any ports in the ODRC's firewall. On occasion, to allow live monitoring, port [redacted] may require opening to access and utilize the customer GUI (graphical user interface).

9. Telephony Services

Voice Services – VoIP

The State of Ohio hosted cloud VoIP service, also known as NGTS (Next Generation Telephony Service) provides core telephony, voice mail, e911, collaboration, video, audio, conferencing and auto attendant functions. Optional services include automatic call distributor (ACD), interactive voice response (IVR), multi-channel contact center solutions and session initiation protocol (SIP) trunking among a variety of other features. The service was the first business class phone system to offer closed captioning for the hearing impaired, and also includes features for those with vision and mobility impairments. The following voice services are offered in addition to the State's hosted VoIP service:

Toll-Free Services:

A service provided to incur telephone charges for incoming calls to an 8xx number.

Automatic Caller Navigation and Contact Center Services (ACD/Contact) Centers:

Contact Center Enterprise allows callers to fill in CRM forms with information prior to an agent responding. With IVR and Advanced Data Collection, callers will spend less time in Call Queues. However, during high demand times, callers can be put on Virtual Hold allowing callers to receive a call back when agents become available. Call recording with screen capture allows the User to monitor, record, store, and QA calls, helping insure a consistent service experience.

Service also includes multi-channel communications including chat, text, SMS and email to afford those trying to contact the State the ability to contact the State in a variety of ways.

Call Recording Services:

Call Recording Services for new VoIP profiles or modifying existing profiles.

Conferencing

This service offers a conferencing service via telephone lines. It provides voice conferencing capabilities within the network and participants can also join in from outside the network.

Fax2Mail:

Fax2Mail is a "hosted" fax solution that allows organizations to seamlessly integrate inbound and outbound fax with their existing desktop email and back-office environments. Fax2Mail is completely "cloud-based" (SaaS), providing an easy to implement, easy to manage solution requiring no expenditures on hardware or software. Fax2Mail solves all faxing requirements, including inbound and out-bound fax, both at the computer desktop and from/to back-office systems, ERP applications, and electronic workflows.

Session Initiation Protocol (SIP) Call Paths:

Session Initiation Protocol Call Paths is used to allocate bandwidth. SIP Call paths:

- Provide existing telephony infrastructure with NGTS services.
- Extends infrastructure into the NGTS cloud.
- Leverages existing investment.
- Bridges the gap.
- All of the United States are Local Calls.
- Share video and collaboration.
- Leverage Toll Free offering.
- Centralized trunk savings.

Site Survivability:

Provides reliable communications via multi-feature redundancy for centralized call processing.

VoIP related Professional Services and Training:

Training services can be requested for VoIP telephone Users.

Professional services are also available for planning and migration of large contact centers, and for integration of contact centers with cloud services including Salesforce.

Please explain how the State's Voice/VoIP Services will be incorporated into the proposed solution. If this section, or portions of this section, are not applicable, please explain and note as N/A. Please note that any proposed variances must be noted in Appendix A – Request for Variance to State IT Policy, Standard or Service Requirements. The language within the supplement shall not be modified.

GTL Response: Not applicable.

GTL is the exclusive provider of our Inmate Telephone System (ITS) **call processor**, which is designed, manufactured, and maintained by GTL. Each call processor is built and customized by GTL to meet the exact needs of each our clients and offers an unmatched range of benefits to its users. GTL's centralized platform allows system servers to be housed and maintained at GTL's Data and Network Centers.

GTL's centralized ITS solution includes physical call-processing hardware and corresponding network hardware and circuits, designed specifically for the needs of each correctional facility. With this true end-to-end solution, GTL can transmit data over a packet-switched network to continuously back up all call records to our offsite data centers, stream live calls directly to remote investigators, and access phone company databases for highly detailed call validation of every call.

All call traffic is carried via Voice Over Internet Protocol (VoIP) to the GTL data center.

GTL ITS Design and Architecture

GTL's Inmate Telephone System is a Web-based, hosted system that includes all equipment, hardware, and software—including the telephone network, recording system, call-control system, telephones, workstations, printers, and associated software. This solution uses cutting edge call-processing and data-management technology that is designed specifically to operate with the highest degree of reliability in the challenging environment of the corrections industry.

GTL's ITS Solution takes full advantage of ***open architecture*** and state-of-the-art hardware and network design that allow the inmate phone system to be interfaced with other facility systems and easily expanded, upgraded and adapted to accommodate changes in the industry and client requirements. Any new facilities can be networked to existing facilities with the new facility's records added to the common database with no disruption or impact on service to existing facilities.

GTL ITS System Architecture

[redacted]

Appendix A – Request for Variance to State IT Policy, Standard or Service Requirements

If an offeror needs to request a variance from a State IT Policy, Standard or Service requirement outlined in this supplement, please provide a rationale and an overview for each request in the table below.

Section Reference	IT Policy, Standard or Service Requirement	Rationale for Proposed Variance from Requirement	roposed Variance Overview
Example: **Section 3.3.2 Application Services - Enterprise eSignature Service**	**Example**: The offeror shall use the State's eSignature solution.	**Example:** An eSignature solution is already integrated into the proposed solution. Using the State's service would result in increased cost due to integration complexities, as well as additional testing and resource needs. It would also result in longer deliverable timeframe.	**Example:** The Offeror's eSignature solution provides the same capabilities as the State's required solution. The Offeror's solution includes a workflow component and an eSignature User interface.