Ohio | Department of Job and Family Services

John R. Kasich, Governor
Cynthia C. Dungey, Director

July 25, 2017

Dear Vendor:

This letter is to announce the release of the Ohio Department of Job and Family Services (ODJFS) Request for Information (RFI) number JFSR1819048139 for the purpose of obtaining information on effective, secure, and innovative methods and/or modern technologies currently available that provide a single solution for a service model that defines, structures, and automates the flow of work for the following services: human resources, civil rights, ADA request management, language interpretation services, facility operations, forms management, warehouse management, asset management and business services. ODJFS releases this RFI for the purpose of identifying vendors that offer any products, methods and services for the State's consideration in its process to determine whether an investment in a single solution is cost effective and warranted.

If your organization is interested in submitting a response for this project, please obtain the RFI through the ODJFS web site at http://www.jfs.ohio.gov/rfp/. In the event of any problems accessing this document or opening the above referenced ODJFS URL, please contact the RFP/RLB Unit at (614) 728-5693.

Responses must be prepared and submitted in strict accordance with the requirements and time frames given in the RFI. Thank you for your attention to this request.

Sincerely,

Jay Easterling
Deputy Director
Contracts and Acquisitions

30 East Broad Street
Columbus, Ohio 43215
jfs.ohio.gov

Ohio Department of Job and Family Services (ODJFS)

Request for Information (RFI): JFSR1819048139

Employee Business Services Modernization Project

Section I – General Information

The Ohio Department of Job and Family Services (ODJFS) is responsible for developing and supervising the State's public assistance, workforce development, unemployment compensation, child and adult protective services, adoption, child care and child support programs. As a support office within ODJFS, the Office of Employee and Business Services (OEBS) and its bureaus support accurate and timely administrative services to the program areas within the Department. These OEBS internal services include human resources, civil rights, American Disabilities Act (ADA) request management, language interpretation services, facility operations, forms management, warehouse management, asset management and business services. The OEBS customer population spans across all ODJFS employees, clients, service providers, county agencies, and citizens of Ohio.

ODJFS releases this Request for Information (RFI) for the purpose of obtaining information on effective, secure, and innovative methods and/or modern technologies currently available that provide a single solution for a service model that defines, structures, and automates the flow of work for the following services: human resources, civil rights, ADA request management, language interpretation services, facility operations, forms management, warehouse management, asset management and business services. Having this information will assist the State to gain a better understanding of prices, products, and number of firms, individuals or organizations (referred to collectively in this RFI as 'vendors') who have a "single tool" solution for OEBS use in improving service level effectiveness of the internal services administered to ODJFS. Accordingly, ODJFS is releasing this RFI to vendors that offer any products, methods and services for the State's consideration in its process to determine whether an investment in a single solution is cost effective and warranted.

ODJFS would like to review and consider available options for a single tool solution. ODJFS also seeks specific information on costs associated with the use of such methods, and pricing structures used by firms that can provide those improvements to government agencies.

Suggestions and comments related to the project as described in Section III of this RFI from vendors who offer products or services that provide a service model that defines structures and automates the flow of work are invited. The objective of this RFI is to gather information from vendors that meets the objectives and specifications defined in this RFI. ODJFS will then consider the responses to this RFI in its decision to make cost-effective improvements to OEBS current processes to manage and provide internal services.

Responses that are alternatives which fall outside of the parameters listed, but could achieve the stated goals of the project, are welcome. ODJFS recognizes the depth of knowledge and experience present in the vendor community that could provide valuable information to help in the State's assessment of its current processes. This RFI is an effort to draw on that expertise.

If ODJFS learns of the existence and availability of multiple cost-effective methods and technologies for enhancing its ability to provide human resources, civil rights, ADA request management, language interpretation services, facility operations, forms management, warehouse management, asset management and business services, and decides to acquire such services and/or products, a formal competitive procurement opportunity will be developed and released in order to identify the vendor most capable of fulfilling ODJFS' specific needs at the most reasonable cost. In that event, the solicitation would be open to any vendor that meets the requirements that would be defined in that solicitation, and participation in this RFI process would NOT be a requirement. Also, whether any vendor decides to respond to this RFI will neither increase nor decrease that vendor's chances of being awarded a contract from any competitive solicitation, if any is subsequently made.

However, if ODJFS determines that inadequate competition among vendors offering such methods, technology, and/or services currently exists to warrant a formal competitive procurement opportunity, but a single solution is identified through this RFI or other means, ODJFS may decide to negotiate a contract with the vendor offering that solution.

IMPORTANT: Vendors are prohibited from including any trade secret information as defined in Ohio Revised Code (ORC) 1333.61 in response to any ODJFS procurement effort. ODJFS shall consider all responses voluntarily submitted to any ODJFS procurement document to be free of trade secrets, and such responses if opened by ODJFS will, in their entirety, be made a part of the public record**.**

RFI Clarification Process – Questions and Answers

Interested parties may ask clarifying questions regarding this RFI, using the following Internet process:

- **Access the ODJFS Webpage at http://jfs.ohio.gov;**
- **Select "Doing Business with ODJFS" from the bottom of the page;**
- **Select "RFP's" from the left side column;**
- **Select Number JFSR1819048139 from the list of competitive opportunities;**
- **Follow the link to the dedicated webpage;**
- **Select "Submit Inquiry" near the bottom of the webpage;**
- **Follow instructions there for submitting questions; or, to view posted questions and answers;**
- **Select "View Q and A" near the bottom of the webpage.**

In submitting a question, please provide the contact person's name, the organization's name, e-mail address, and business phone number. ODJFS will not respond to questions submitted after 8:00 a.m. on the date the Q&A period closes, as identified in the following timetable.

Questions will be answered only if they are submitted using this process, and are received before the close of the Q&A period. ODJFS' responses to all questions asked via the Internet will be posted on the webpage dedicated to this RFI for public reference by any party.

Should vendors experience technical difficulties accessing the ODJFS website where the RFGA and its related documents are published, they may contact the ODJFS Office of Contracts and Acquisitions (OCA), at (614) 728-5693 for guidance.

Anticipated Timetable

DATE	EVENT/ACTIVITY
7/26/2017	ODJFS releases the RFI to the Vendor Community on the internet: Q&A period opens -RFI becomes active; vendors may submit inquiries for RFI clarification.
8/14/2017	Q&A period closes; 8 a.m. -No further inquiries will be accepted.
8/21/2017	**Deadline for Vendors to submit responses to ODJFS, 3 p.m.**

Section II – Project Background

OEBS utilizes several individual tools to facilitate service offerings for the following services: human resources, civil rights, ADA request management, language interpretation services, facility operations, forms management, warehouse management, asset management and business services. OEBS is looking for a single tool solution to improve its administration of these organizational and internal services and replace outdated tools.

Section III – Outline of ODJFS Needs and Specifications

The purpose of this RFI is to gather information on the range of vendor solutions that could improve the OEBS' facilitation of its organizational and internal services provided to ODJFS. ODJFS is particularly interested in any potential solutions in which a single tool implements a service model that defines structures and facilitates automated workflows, ticketing, case management, auto notification, tracking, archiving, and capability to interface with ODJFS system.

Vendors that respond to this RFI are encouraged to identify any additional system features that could prove beneficial in facilitating the aforementioned organizational and internal services OEBS provides to ODJFS.

The following Solution Criteria provides high-level descriptions of ODJFS solution requirements. Refer also to supporting categorical requirements described in the RFI attachment, "RFI Section III Solution Criteria – Supporting Requirements".

Solution Criteria:

A. **Attachments**: The system should have the ability to add attachments. It is imperative that the ability to attach files be included to all necessary and applicable functions within the system. This function is a requirement for all of OEBS' business lines, pertinent to record keeping, warehousing, asset and case management. The ability to add attachments electronically will ensure that all required records are stored, maintained and preserved throughout the interactive processes as well as for retention purposes.
    1. There should be no limit in the number of attachments (knowing that the total size of all documents could come with limitations, specifically with the Database backend).
    2. The attachments can and should support any file type (i.e. doc, excel, pdf, jpeg, tiff, bmp, mpeg etc.), without any limit.
    3. File names should be searchable within the system, and should show some sort of relationship to the record it is attached to (i.e. ticket, asset, case, etc.).
B. **Dashboard:** The system must have the ability to display "quick stats" of items and/or records being tracked (tickets, assets, cases, etc.), called Dashboards. These stats need to show what ODJFS would deem "important." The expectation is that dashboards are completely configurable, with the ability to reflect any data point that is being tracked on each record. Dashboard designs must be flexible to be viewed in many different formats such as, but not limited to: pie graphs, bar graphs, donut graphs, line graphs, etc. Dashboards must be drill-down capable.
    1. These can be based off reports. Reports may be the base of each of these dashboards wherein the user creates a report, which is then converted into a dashboard, but this is not a necessity.
    2. Dashboard access to the actual dashboards, as well as access to the data they are pulling from, need to be permission/role/rights based, so that individual users and/or groups of users can be given rights not only to see a dashboard, but being able to pull data from specific types of records.
    3. Drill-down refers to the ability to open data that is more refined by clicking on any section. Drill-down also refers to the ability to open a group of tickets/records/assets that are reflected by the graph being clicked on.
C. **E-Approval**: The e-approval functionality would consist of an electronic sound, symbol, or process attached to or logically associated with a record and executed or adopted by a person with the intent to sign and/or approve a record or action (i.e. Asset Management Assignments, Budget, Forms, Maintenance Sign-offs, etc.).
D. **Functionality**:
    1. **Ad-Hoc Custom Fields:** Must have the ability to create custom fields for OEBS use, that are searchable, reportable, printable, etc.

2. **Asset Management Self-Service:** The system must have a screen/form that is accessible by any user with proper identification & password allowing them to take specific actions on any tagged asset(s), search for any tagged asset(s), and run reports against their search results.
    a. Users need the ability to take an action (such as, but not limited to: sign for asset, verify asset, update address, etc.).
    b. This should also give them the ability to search for any asset (by Tag Number, or Serial Number), search for people assigned asset(s), search by location, and search by Office (within this agency).
    c. They would also have the ability to run a report on their search results, and have a way to toggle between their assigned assets, the asset search screen, and assets they have signed for.
    d. When taking an action, the ability to apply any action (or multiple actions) to multiple different assets, all at the same time is mandatory. The system will record anything the end user does, as well as write the date/time and ID/Name of said user to specific fields ODJFS/OEBS uses for yearly asset verification.
    e. The system will allow users to verify/sign for their assets on a yearly basis; the time/date this is done needs saved directly to asset.
3. **Asset Salvaging:** The system should also support a method of salvaging, specific to Asset Management, to potentially utilize a unique date requirement (Julian calendar). The system will also have an approval system, to allow only specific people (and/or groups) to perform the action of salvaging approval.
4. **Bulk Data Imports:** Bulk Data Imports must be supported. This is done by way of importing spreadsheets housing all the data points needed by the system. After imported, this data is staged on a form that is internal to the system for validation. After data is validated, the spreadsheets are approved for processing. Lastly, data processing is checked for errors. This is all done via one single form. This same process must be similar, if not improved, by a new asset management system.
5. **Check In/Out:** Inventory check in and check out is needed by the system, as well as keeping track of inventory counts as items are removed and/or replenished.
6. **Data Segregation:** The system must ensure data access is only given to those who ODJFS specifies. This is typically done via "multi-tenancy." ODJFS needs to ensure that not all users of the same system can see all records. An example of this would be: two companies (ABC & XYZ) have access to the same ticketing system. Neither of these companies can view the other company's tickets (ABC cannot see tickets opened for XYZ and vice versa). A manager of both companies CAN view either company, or both at the same time.
7. **Electric Form Creation:** The system must have the ability for administrators to generate electronic forms dynamically as needed with approvals. Either development of a form specific to our needs or a report that can mimic this form close enough to suffice the needs of OEBS. The form must also support electronic signatures.
8. **Email Inbound/Outbound:** The system must support the use of multiple different Outlook/Exchange mailboxes for use of inbound and outbound correspondence. A particular mailbox needs to be used for different functions, as well as different types of users within the same function. All outbound emails must be recorded and associated within the system record. Inbound emails should be automatically recorded by the

system (just like outbound), processed without user intervention, and recorded in this same record (using notifications so the user knows an inbound email has been received by the system).

   a. The mailbox used needs to be dependent on what module within the system is being used, and what type of data within that particular module is being used as well (defined as 'multiple tenants').
   b. The "from" field of outbound emails should reflect the system being used, as well as the data access currently assigned.
   c. A logged in user's (sender) personal/identified email address should not be exposed via email (i.e. from field).

9. **Historical Audit Log:** All actions taken on any record are time and date stamped along with the user name (and/or User ID) of the logged in user making said changes. There should be a log that can be referenced, as well as searched and reported against at any given time.
10. **Integration:** The system must integrate into existing state systems such as (PeopleSoft-OAKS, and Microsoft Active Directory) so records are automatically created and disabled, when parent system changes (for example through a nightly sync).
11. **Knowledge Management:** OEBS needs the ability to store documents in which the contents of said documents are fully searchable, referenceable, and can be categorized. Knowledge management entries must support RTF, Unicode, HTML (in terms of verbiage being copied from a website into a Knowledge article, as well as URL references), and any other kind of standard text formatting. Knowledge management must also support the uploading of existing documents.
    a. Knowledge management entries need to be able to be associated to a record (ticket, asset, case, etc.), and can be for the purpose of the creator's imagination (i.e. checklists, troubleshooting steps, process flow, etc.).
    b. The ability to create folders is desired, but can be offset by using other means such as, but not limited to tags, categorizations, relationships, etc.
12. **Maps:** OEBS would prefer dynamic interactive graphical representation of requests throughout all supported sites throughout the entire state. A site map would suffice, so long as it shows the granularity of site/building, floor, room/area. Further granularity would be desired.
13. **Overview Screen:** Overview screen/form is needed for each module with the system (ticket, case, asset, etc.). This one "overview" screen will have the ability to show all tickets that meet a particular search and/or filter criteria. This same overview will provide key fields to further filter.
14. **Printing:** Simple ad-hoc print feature must be available while within a record. Every data point can be printed as part of a report.
15. **Purchase Order Cross-Reference:** The system must support a mechanism to pull in Purchase Order (PO) data from a different system (using an intermediary Windows server), and allow matching of PO line items to a single asset. For example, if 5 chassis', 5 hard drives & 10 sticks of RAM are purchased, the system needs to allow for 1 chassis, 1 hard drive & 2 sticks of RAM to be associated to one asset. The system will need to match PO line items 4 more times to account for 5 assets in total.
16. **Record Assignment:** The system must be able to assign and reassign any record to any group and/or user of the system. Specific to Asset Management, the system must have

the ability to assign an asset to anyone in the PeopleSoft database, not only users of the system ("users" refers to those who get assigned records and work records to their resolution). The system must also be able to see previously assigned people/users (historical info). All this assignment (Group/User) must be visible from the currently opened record.

17. **Record Entry Methods:** The system must support multiple methods of record entry (aside from the more conventional manual record entry), namely automated methods. Records must be able to be auto-created based on emails coming into a designated mailbox.
    a. A desired entry method would be inbound faxes to a designated phone number, although this can be mitigated through internal process changes.
    b. The system must support the intake of requests coming from outside the ODJFS internal private network.
    c. Newly created records need to be auto-assigned to a specific group, based on the creation method or by criteria defined upon manual ticket creation.
    d. The system must be flexible enough to automatically create tickets from either any inbound inquiry, or by specific inbound inquiries (i.e. specifying a specific email address that the system will only recognize, or from any inbound email address and/or domain).
18. **Relationships:** General use of relationships between modules and within the same module. Relationships (Parent/Child as well as Sibling) will be needed for ad-hoc use. Additional relationships are preferred. The system must have the ability to know what types of items are related to a user that must follow said user on a relocation request.
19. **Scheduling:** Scheduling for follow-up items is also desired, as well as historical records of these activities. Furthermore to schedule actual "down time" for assets, facilities, etc., so users know they cannot be used at that time.
20. **Self-Service:** Any user should have the ability to create a record (excluding an asset) or request a record be created. Users should have the ability to request changes to an existing record, but not to make the changes themselves (other than their time/date/ID stamp of electronic signatures).
21. **Simplified Data Entry:** When entering data for initial record creation, ODJFS would prefer to have all data points on one single screen, rather than using multiple tabs to house all data fields available. This would not have to be the only entry point, leaving a tabbed solution still viable for others to use.
22. **Simultaneous Updates**: The system must allow for multiple (no limit) assets to have the same updates made across all selected. One change to any available data field, to any/all assets.
23. **SQL Queries:** The system must support the use of standard SQL queries, so multiple data points and criteria can be used in search of records.
24. **Templates:** The system must support multiple facets of templates. One expectation is that templates would be available for use with email correspondence, so that identical emails can be sent by different users, in different scenarios, creating a uniformed email being sent regardless of who the sender is. Another expectation for use of templates would be for uniform record creation.
    a. Variables must also be supported.

i. This refers to the use of variable statements in the email templates so that data elements can be pulled out of a record, to personalize each email. Some examples of email template variables may include: Requestor Name, Record Status, Record Description, etc.

b. When a template is used for ticket creation, some fields would be filled out automatically for the user, so the minimal amount of data entry is needed for initial record submission (i.e. Requestor, etc.).
    i. Templates can make record creation quick and easy, as well as categorize records appropriately and "auto-assign" a record, based on the use of this field in the template and/or based on the categorization used.

E. **History:** The system must be able to maintain a separate archival database for outdated information. Archived information must have the ability to save all actions, comments, and audit trail for historical and retention purposes.

F. **Interface:** The system must have the ability to interface with the Department of Administrative Services (DAS) managed Exchange/Outlook system (or Exchange/Outlook's ultimate source), to synchronize people data. Other interfaces are the ODJFS System Center Configuration Manager (SCCM) source for PC information, as well as other systems. Additional PeopleSoft interfaces needed are OAKS FIN (PeopleSoft) for purchasing details and OAKS AM (PeopleSoft) to push/pull asset info back and forth. The system needs to support data being pushed to the ODJFS internal website. Barcode scanning support is necessary, for handheld wireless scanners, and mobile devices (i.e. Smart Phones). It also must interface with all other modules within this same application (tickets, assets, case, etc.). Desired functionality would allow for location tracking while using geo location, maps, and floor plans.

G. **Mobile:** The mobile functionality would enable the tool to be used on tablets, smart phones, and other mobile devices.

H. **Notification:** The system must automatically provide notifications to both internal and external sources. Many of OEBS listed business lines have stringent timelines and processes making it imperative that notifications be sent from the system to users on a constant basis. Notifications are to include, but are not limited to the following: Notifications informing users when a request is submitted, notifications informing users when requests/cases have been dormant for a fixed time, notifications warning when a purchase order balance is nearing its set amount, etc.

I. **Reporting:** The reporting functionality for the system should have the ability to provide instant, operational data, covering a broad range of needed topics (i.e. ADA Case Management, Asset Management, Budget, Customer Service Surveys, Forms Management, maintenance and move information, etc.). The system must also be able to provide notifications of changes, updates, and alerts for various functions.

J. **Scanners:** The scanners functionality would allow the tool to be integrated with differ type of barcode scanners to easily import or bring up information associated with the barcodes (i.e. Asset tags, forms, printed barcodes, etc.).

K. **Search:** The Search feature should have easy navigation in searching for various data points (i.e. names, tracking numbers, tags, items, equipment, POs and PO details, etc.). All fields should be searchable and reportable allowing sorting/filtering.
    1. In some circumstances, search capability must have the ability to restrict access to sensitive information.

2. Searchable and reportable data must be able to export into other formats (i.e. other systems, excel, pdf, etc.)

L. **Security:** The system must be able to provide secure protections for all information. The system must have the ability to restrict and control all levels of access and authority; including but not limited to creating, modifying and maintaining varying user roles with defined levels of authority. The system must meet the security provisions of the state as referenced in the RFI attachment "DAS Security Requirements_ODJFS14001_Supplement Two_136" and the RFI attachment "IDAM RFP requirements_136."

M. **Self Service – Customer Request Portal:** The self-service portal should be able to allow varying degrees of access to the system to allow ODJFS employees to enter maintenance, move, and other types of service requests. The functionality must be able to allow for approval, resourcing of information, and the assignment of the task to individuals or groups of employees. Similarly, a workflow must be created with the capability of producing a document or request for those outside of the project's reach (i.e. third party vendors, property managers, etc.).

N. **Single Sign-on:** The system must, for State employees, businesses and citizens, provide single sign-on capabilities through integration with the State's Enterprise Identity Management system. Refer to RFI attachment, "Identity Access Management" for additional information.

O. **State Standards:** Refer to RFI Appendix II, "Supplement Two", the requirements described therein shall apply to any and all Work, Services, Locations and Computing Elements that the Vendor will perform, provide, occupy or utilize in conjunction with the delivery of work to the State and any access of State resources in conjunction with delivery of work.

P. **Ticketing:** The ticketing functionality should register an event or a ticket, assign an owner, or person responsible to the ticket, assign additional interested parties to the ticket, track changes to the ticket, inform interested parties of these changes, launch activity based on ticket status and/or priority, report on status, and close the ticket.

Q. **Tracking:** The tracking functionality for the system should have the ability to maintain and update files and information for all types of databases (facilities, people, records, forms, leases, invoices, etc.). The system must have the functionality to track all requests, forms, assets, etc., including but not limited to all data elements, asset information, status updates, and inventory. This function is a necessity as it is essentially important for information to be readily available, and amendable. Unique identifiers are needed in all records. Similar to the use of a Serial Number as a unique identifier, but this would be specific to the system (the system's own unique identifier for each record).

R. **Tracking History & Archive:** The tracking capabilities should include the capacity to easily pull the history of an asset or item, including every stop along its path to its current location, complete with dates, locations, etc. Tracking must also include the capability to archive assets that have been disposed of, so that they do not appear in certain reports.

S. **Workflow:** The ability to create workflows would allow the execution and automation of business processes where tasks, information and documents are passed from one participant to another for action, according to a set of procedural rules (i.e. procedural rules for: Asset, Records, Inventory, ADA Case, Forms, Space, Budget, and Facilities Management, etc.).

Section IV - Content and Format of Response

General Response Guidelines:

A. Responses should be limited to twenty-five (25) pages in length, including any charts, graphs or information display tools.

B. Responses should briefly describe the vendor's organization, including its products and services and its industries and customers.

C. Responses should briefly describe the product or services it could provide or develop in order to meet the ODJFS needs referenced in Section III, and provide a description of the proposed approach to meeting the State's need for such a "single tool" solution.

D. Responses should provide an estimate of the implementation or start-up timeline for the proposed product/service for any new customers.

E. If the suggested solution or approach is technology-based, responses are to describe any technological requirements, contingencies, and prerequisites for ODJFS for the solution's implementation.

F. Responses should describe any training that would be necessary for ODJFS staff, detailing the likely length, mode, and location of the training.

G. Responses should provide cost estimate by the following categories: software licensing description and cost, hardware costs, proposed implementation services hourly rates by job title, training costs and any other pertinent costs to allow for analysis by ODJFS.

Responses to this RFI are to be submitted electronically (in a secure .PDF document format) to the following e-mail address: OCA_QUESTIONS@jfs.ohio.gov

Thank you for your efforts to provide ODJFS with your suggestions, comments and relevant information to assist with this project.

Identity Access Management

Identity Management Strategic Approach to Access Control also known as IDAM project will provide a secure digital identity experience including an intuitive and interactive user experience for Ohio's citizens, businesses, and employees. The program provides centralized administration and synchronization of user identities to enable user provisioning and de-provisioning of identity and access for state systems. The requested technology must provide State employees with single sign-on capabilities through integration with the State's Enterprise Identity Management system.

Program delivery is aligned around four distinct pillars that support a consistent user experience for State of Ohio services constituents:

Enterprise Identity Pillar: Enterprise ID Management Framework having the following capabilities:

- User Provisioning
- Single Sign-on
- Identity Proofing
- 2-Factor Authentication (2FA)
- Federation
- Logging and Monitoring

Fraud and Risk Analytics Pillar: A comprehensive, risk-focused fraud detection and analytics service that can detect, prevent, analyze, and report on fraudulent activities in real time.

This enterprise, thin-layer tool is built upon the Federal Data Science Framework and provides:

- Continuous Machine Learning
- Scalable and Accessible Big Data
- Real-time Detection
- Key Graphics

User Experience Pillar: The User Experience Pillar supports an enhanced user and agency experience through consistent look and feel, optimized flows and functionalities and reduced redundancy.

- **User Interface:** (To the extent possible) standardized look and feel, navigation, and presentation of web sites, portals, and applications using a standard digital interface.
- **User Experience:** User-centric design, processes, tasks, and functions that support quicker, easier, and more secure access to and interaction with state agencies.
- **Agency Experience:** State-wide, centralized access point that adheres to the desired user experience and user interface, supported by standard tools, methods, and digital tool kits.

Platform and Portal Services Pillar: Provide an experience that promotes privacy, choice, and flexibility for citizens, businesses, and employees by:

- Enabling better, more secure access to an ever-growing set of digital services and self-help features across the state through a single proofed identity
- Enabling the state as an organization to consolidate historical transactions and cross-program / agency data to lead a better user experience

An internal DX Portal acts as the platform by which portal services are provided to agencies. The service portfolio includes:

- Design
- Personalization
- Multitenant and Enterprise Hosting
- Portal and Application Cloud Deployment Control
- Portal Framework
- Integration
- Content Management
- Portlet and Service Consumption and Publishing

Required Interfaces with IDAM:

Federated Single Sign-on: Application must support federated single sign-on using SAML 2.0 Tokens for identity assertion to authenticate the user to the Application.

Authorization-Based Assertion Attributes: Application, optionally but preferred, would support SAML 2.0 Token assertions to determine appropriate authorizations (roles/permissions) for the individual, upon sign-in, based upon supplied SAML attribute(s) (such as group memberships).

Automation of Provisioning / de-provisioning: Application must support either:

1. A connector that is available within the IBM Identity suite to automate Agency provisioning and de-provisioning tasks.
2. The Application has SOAP or REST Service(s) available that the IBM Identity suite can call to automatically perform provisioning and de-provisioning tasks.

Provisioning Tasks that must be available:

- Create, or associate, an identity in the application for authentication and single sign-on.
- Assign and Change an identity's assignment to specific Roles/Permissions within the application for authorization.

De-provisioning Tasks that must be available:

- Delete, or un-associate, an identity in the application to revoke the person's ability to authenticate.
- Remove or alter specific Roles/Permissions per identity within the application to remove authorization(s).

Supplement Two:

State Architecture and Computing Standards Requirements

State Security and Privacy Requirements

State IT Computing Policy Requirements

State Data Handling Requirements

Contents

1. Overview and Scope

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 of State resources in conjunction with delivery of work.

This scope shall specifically apply 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 agreement;
- 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 confidential, personal, financial, infrastructure details or sensitive data.

The terms in this Supplement are additive to the Standard State Terms and Conditions contained elsewhere in this agreement. In the event of a conflict for whatever reason, the highest standard contained in this agreement shall prevail.

2. State Architecture and Computing Standards Requirements

2.1. Requirements Overview

Offerors responding to State issued RFQ / RFP requests, and as Contractors performing the work following an award are required to propose solutions that comply with the standards outlined in this document. In the event of a conflict with any published Standard, a variance may be requested, and the Offeror must show sufficient business justification for the variance request. The Enterprise IT Architecture Team will engage with the Contractor and appropriate State stakeholders to review and approve / deny the variance request.

2.1.1. State of Ohio Standards

The State has a published Core Technology Stack as well as Enterprise Design Standards as outlined in this document and, due to State preferences, are subject to improvements and change. The State also provides numerous IT Services in both the Infrastructure and Application categories, as outlined in the State's IT Services Catalog at: http://das.ohio.gov/Divisions/InformationTechnology/StateofOhioITServiceCatalog.aspx

2.1.2. Offeror Responsibilities

Offerors can propose on-premise or cloud-based solutions. When proposing on-premise solutions, vendors must comply with State requirements including using the State's Virtualized Compute Platform. Unless otherwise specified in the RFP, offerors proposing on-premise solutions are required to install third party applications on State provided compute platforms. Dedicated server platforms are not compliant with the State's Virtualization Requirements.

Hardware and storage (memory, speeds, cpu and other configuration details) should be proposed to adhere to established State standards (generally VMware based system images for x86 environments) and or virtualized Oracle Exadata/Exalogic frames and components unless otherwise specified in the RFP.

In addition, Offerors are required to take advantage of all published IT Application Services where possible, i.e. Enterprise Service Bus, Content Management, Enterprise Document Management, Data Warehousing, Data Analytics and Reporting and Business Intelligence. When dedicated Application components are required, i.e. Application Servers, Databases, etc., they should comply with the Core Technology standards.

2.1.3. State Infrastructure Services

The State of Ohio's Office of Information Technology Infrastructure Services Division (OIT/ISD) will be responsible for providing the technical infrastructure platform as a service to the Contractor and will host the Contractor developed software and operating solution following the conclusion of the project for on-premise solutions. In general, this service includes the following:

- Primary Computing Facility: State of Ohio Computing Center (secure Tier III capable facility)
- Alternate/Disaster Recovery Center: Ohio Based Secure Tier II facility
- Redundant Networking between State facilities and Data Centers (Metro-E to 10Gb/s OARnet)
- Physical and Infrastructure Security Services
- Redundant Power, Cooling, Fire Suppression and onsite Redundant UPS/Power Generation
- Servers, Storage, Networking Devices, Firewalls, Security Appliances, Vulnerability and Virus Scanning to the operating system prompt
- Binding SLAs regarding performance, availability, reliability, provisioning and systems administrative access

The State of Ohio will provide ITIL based services in support of the Contractor as follows:

State Infrastructure Responsibility Matrix	
Asset Management ▪ Hardware Asset Tracking ▪ Software Asset Tracking ▪ Logistics Support ▪ Inventory Capture and Maintenance **Service Desk** ▪ Help Desk Operations ▪ Help Desk Tools ▪ Service Desk Processes	**Enterprise Security Management** ▪ Emergency Response Service ▪ Threat Analysis ▪ Managed Intrusion/Detection/Prevention ▪ System Security Checking ▪ Security Advisory and Integrity ▪ Malware Defense Management ▪ Vulnerability Management ▪ ID Management ▪ Security Policy Management ▪ Security Compliance Support ▪ Security Audit
Server Management ▪ Platform Support (Tools/Processes Procedures) ▪ Unix/Intel Servers ▪ Incident Management ▪ Server Operations ▪ High Availability ▪ File Management **Storage Planning** ▪ Capacity Management ▪ Storage Performance Management	**Data Center and Wide Area LAN/WAN Management** ▪ Enterprise Internet Services ▪ Regulatory/Change Management ▪ Network Engineering ▪ Standards ▪ LAN/WAN Management ▪ Network Operations and Management ▪ Network Capacity/Availability Management ▪ Network HW/SW Management ▪ Network Security ▪ Network M/A/C/D
Data Center Architecture Planning ▪ Hardware/Facilities Planning ▪ Unix/Intel Servers ▪ Platform Configuration Management ▪ Performance Management ▪ Capacity Management ▪ Batch Operations/Scheduling ▪ Storage Management ▪ Backup/Restore ▪ Media Management, Media Operations, Offsite Storage	**Data Center Facilities Management** ▪ Site Maintenance and Operations ▪ Site Availability Management ▪ Routine Maintenance and Upgrades ▪ Non-Technical Services (parking lot, landscaping, snow removal etc.)

2.2. Compute Requirements

2.2.1. Client Computing

Offerors must not propose solutions that require custom PC's, Laptops, Notebooks etc. Unless otherwise specified in the RFP, the State will source its own Client computing hardware and the Offeror's proposed solutions are required to be compatible with the State's hardware.

2.2.2. Server / OS

Offerors must propose solutions that comply with the State's supported Server Operating Systems (OS).

The following are the State's Required Server Operating Systems.

Table 1 – Supported Server OS

Microsoft Windows Server	Standard, Enterprise, & Datacenter
RedHat Linux	Enterprise
SUSE Linux	Enterprise
IBM AIX	
Oracle Enterprise Linux	Enterprise

When Offerors are proposing on-premise solutions, these solutions must comply with the State's supported Server Compute Platforms.

The State hosts and manages the Virtual Server hardware and Virtualization layer. The State is also responsible for managing the server's Operating System. This service includes 1 virtual CPU (vCPU), 1 GB of RAM and 50 GB of Capacity Disk Storage. Customers can request up to 8 vCPUs and 24GB of RAM.

For Ohio Benefits and the Ohio Administrative Knowledge System (OAKS) – Exalogic

2.2.3. Ohio Cloud: Hypervisor Environment

When Offerors are proposing on-premise solutions, these solutions must comply with the State's supported VMware vSphere, and IBM Power Hypervisor environment.

For Ohio Benefits and OAKS – Oracle Virtual Manager, Xen

2.3. Storage and Backup Requirements

2.3.1. Storage Pools

The State provides three 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.

When Offerors are proposing on-premise solutions, these solutions must take advantage of the State's Storage Service Offerings.

For Ohio Benefits and OAKS - HA (High Availability) storage used with Mirror configuration.

The pools and their standard use cases are below:

Table 2 – State Supported Storage Pools

Performance	Highest	Fast	Performance pool suited for high availability applications, with high I/O (databases).

General	High	Fast	General pool suitable for file servers, etc.
Capacity	High	Average	Capacity pool suitable for file servers, images and backup / archive). Not suited for high random I/O.

2.3.2. Backup

When Offerors are proposing on-premise solutions, these solutions must take advantage of the State's Backup Service Offering.

Backup service uses IBM Tivoli Storage Manager Software and provides for nightly backups of customer 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 for customer data. OIT backup facilities provide a high degree of stability and recoverability as backups are duplicated to the alternate site. All critical production systems must also use the State's DR facility.

For Ohio Benefits - Symantec NetBackup is the Enterprise backup solution.

2.4. Networking Requirements: Local Area Network (LAN) / Wide Area Network (WAN)

Offerors must propose solutions that work within the State's LAN / WAN infrastructure.

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 and Local Government.

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

The State provides a high bandwidth internal network for internal applications to communicate across the State's LAN / WAN infrastructure. Normal traffic patterns at major sites should be supported.

Today, the State's WAN (OARnet) consists of more than 1,850 miles of fiber-optic backbone, with more than 1,500 miles of it operating at ultrafast 100 Gbps speeds. The network blankets the state, providing connectivity to all State Government Agencies.

The State of Ohio Network infrastructure utilizes private addressing, reverse proxy technology and Network Address Translation (NAT). All applications that are to be deployed within the infrastructure must be tolerant of these technologies for both internal product interaction as well as external user access to the proposed system, infrastructure or application.

The State Network team will review applications requirements involving excessive bandwidth (i.e. voice, video, telemetry, or applications) deployed at remote sites.

2.5. Application Requirements

2.5.1. Application Platforms

When Offerors are proposing on-premise solutions, these solutions must be developed in open or industry standard languages (e.g. Java, .NET, PHP, etc.)

2.5.2. Open API's

Proposed vendor applications must be developed with standards-based Open API's. An open API is an application program interface that provides programmatic access to software applications. Proposed vendor applications must describe in detail all available features and functionality accessible via APIs.

2.5.3. SOA (Service Oriented Architecture)

When Offerors are proposing on-premise solutions, these solutions must be developed using a standards-based Service Oriented Architecture (SOA) model.

2.6. Database Platforms

Proposed vendor application designs must run on databases that comply with the State's supported Database Platforms.

- DB2
- SQL
- ORACLE
- Exadata

2.7. Enterprise Application Services

The State of Ohio Office of Information Technology (OIT) provides a number of Enterprise Shared Services to State agencies as outline in the IT Services Catalog available at:
http://das.ohio.gov/Divisions/InformationTechnology/StateofOhioITServiceCatalog.aspx

At a minimum, proposed vendor application designs that include the following Application Services must use the Application IT Services outlined in the IT Services Catalog.

2.7.1. Health and Human Services: Integrated Eligibility

The Integrated Eligibility Enterprise platform provides four key distinct technology domains / capabilities:

- Common Enterprise Portal – includes User Interface and User Experience Management, Access Control, Collaboration, Communications and Document Search capability
- Enterprise Information Exchange – includes 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
- Analytics and Business Intelligence – Integration, Analysis and Delivery of analytics in the form of alerts, notifications and reports
- Integrated Eligibility – A common Enterprise Application framework and Rules Engine to determine eligibility and benefits for Ohio Public Benefit Programs

2.7.2. The Ohio Business Gateway (OBG)

The Ohio Business Gateway (OBG) offers Ohio's businesses a time-and money-saving online filing and payment system that helps simplify business' relationship with Government agencies.

- New Business Establishment – Provides a single, portal based web location for the establishment of new businesses in Ohio, file with the required State agencies and ensure that business compliance requirements of the State are met.
- Single Point Revenue and Fee Collection - Manage payments to State's payment processor (CBOSS) and broker payment to multiple agencies while creating transaction logs and Business Customer "receipts".

- One-Stop Filing and Forms - Provides guides and forms to Business Users for complex transactions that have multiple steps, forms and / or filing requirements, and instructs users on procedures to complete the process including Agencies and (if applicable) systems they will need to interact with.
- Scheduling and Reminders - Notify Business Customers of a particular event that is upcoming or past due (Filing due) using a “calendar” or “task list” metaphor.
- Collections and Confirmations – Provides a Payment Card Industry (PCI) certified web-based payment solution that supports a wide range of payment types: credit cards, debit cards, electronic checks, as well as recurring, and cash payments.

2.7.3. Ohio Administrative Knowledge System (OAKS)

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 via myOhio.gov, Enterprise Learning Management, and Customer Relationship Management. Core System Capabilities include (but are not limited to):

Content Management (myohio.gov)

- Centralized Communications to State Employees and State Contractors
- OAKS alerts, job aids, and news
- Statewide Top Stories
- Portal to OAKS applications
- Employee and Contractor Management

Enterprise Business Intelligence

- Key Financial and Human Resources Data, Trends and Analysis
- Cognos driven standardized and adhoc reporting

Financial Management (FIN)

- Accounts Payable
- Accounts Receivable
- Asset Management
- Billing
- eBid
- eCatalog (Ohio Marketplace)
- eInvoicing
- eSupplier/Offeror Maintenance
- Financial Reporting
- General Ledger
- Planning and Budgeting
- Procurement
- Travel & Expense

Enterprise Learning Management (ELM)

- Training Curriculum Development
- Training Content Delivery

Human Capital Management (HCM)

- Benefits Administration
- Payroll
- Position Management
- Time and Labor
- Workforce Administration: Employee and Contingent Workers
- Employee Self-Service
- eBenefits
- ePerformance
- Payroll

2.7.4. Enterprise Business Intelligence

- Health and Human Services Information
    - Eligibility
        - Operational Metrics
        - County Caseworker Workload
    - Claims
    - Long Term Care
- Financial Information
    - General Ledger (Spend, Disbursement, Actual/Forecast)
    - Travel and Expense
    - Procure to Pay (AP/PO/Offeror/Spend)
    - Capital Improvements
    - Accounts Receivable
    - Asset Management
- Workforce and Human Resources
    - Workforce Profile
    - Compensation
    - MBE/EDGE

2.7.5. Enterprise Content Management

Hyland OnBase is the State's Enterprise Content Management system for Document Imaging and Document and Records Management. The service is designed to provision, operate and maintain the State's Enterprise Content Management solution.

2.7.6. SharePoint

Microsoft SharePoint Server portal setup and hosting services is available for agencies interested in internal collaboration, external collaboration, organizational portals, business process workflow, and business intelligence.

2.7.7. IT Service Management

ServiceNow is the State's 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. The IT Service Management Tool provides workflows aligning with ITIL processes such as Incident Management, Request Fulfillment, Problem Management, Change Management and Service Catalog.

2.7.8. Customer/Citizen Relationship Management (CRM)

Salesforce, is the State's cloud-based Customer Relationship Management tool that helps agencies build stronger connections between citizens, employees, governments, services, and the information they need.

2.7.9. Enterprise Geocoding Services

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

2.7.10. GIS Hosting

GIS Hosting delivers dynamic maps, spatial content, and spatial analysis via the Internet. User agencies can integrate enterprise-level Geographic Information Systems (GIS) with map capabilities and spatial content into new or existing websites and applications.

2.8. Productivity, Administrative and Communication Requirements

2.8.1. Communication Services

The State of Ohio Office of Information Technology (OIT) provides a number of Enterprise Shared Services to State agencies as outlined in the IT Services Catalog available at: http://das.ohio.gov/Divisions/InformationTechnology/StateofOhioITServiceCatalog.aspx

At a minimum, proposed vendor application designs that include the following Communication Services must use the Communication Services outlined in the IT Services Catalog.

Exchange

- Exchange Mail
- Office 365
- Skype for Business Instant Messaging & Presence
- Enterprise Vault
- Clearwell eDiscovery
- Exchange Web Services
- Bulk Mailing
- External Mail Encryption
- Outbound Fax
- Mobile devices

EDI/Application Integration/Medicaid EDI

Lyris Listserv

On-premise application-based FAX

eFAX

Fax2Mail is a "hosted" fax solution that allows agencies to seamlessly integrate inbound and outbound Fax with their existing desktop E-mail and back-office environments. Fax2Mail is a "cloud-based" solution.

Voice over Internet Protocol (VoIP)

The CBTS VoIP service, which is open to all agencies, boards, commissions, local governments and state supported education institutions, as well as State of Ohio Cooperative Purchasing Program members, provides core telephony, voice mail, collaboration, video, audio, and auto attendant functions to eligible customers. Optional services including ACR, IVR, Call Center Solutions and SIP Trunking are also available.

3. General State Security and Information Privacy Standards and Requirements

The Contractor will be responsible for maintaining information security in environments under the Contractor's management and in accordance with State IT Security Policies. The Contractor will implement an information security policy and security capability as set forth in this agreement.

The Contractor's responsibilities with respect to Security Services will include the following:

- Provide vulnerability management Services for the Contractor's internal secure network connection, including supporting remediation for identified vulnerabilities as agreed.
- Support the implementation and compliance monitoring for State IT Security Policies.
- Develop, maintain, update, and implement security procedures, with State review and approval, including physical access strategies and standards, ID approval procedures and a breach of security action plan.
- Manage and administer access to the systems, networks, System software, systems files and State data, excluding end-users.
- Provide support in implementation of programs to educate State and Contractor end-users and staff on security policies and compliance.
- Install and update Systems software security, assign and reset passwords per established procedures, provide the State access to create User ID's, suspend and delete inactive logon IDs, research system security problems, maintain network access authority, assist in processing State security requests, perform security reviews to confirm that adequate security procedures are in place on an ongoing basis, and provide incident investigation support (jointly with the State), and provide environment and server security support and technical advice.
- Develop, implement, and maintain a set of automated and manual processes to ensure that data access rules are not compromised.
- Perform physical security functions (e.g., identification badge controls, alarm responses) at the facilities under the Contractor's control.
- Prepare an Information Security Controls Document. This document is the security document that is used to capture the security policies and technical controls that the Contractor will implement, as requested by the State, on Contractor managed systems, supported servers and the LAN within the scope of this agreement. The Contractor will submit a draft document for State review and approval during the transition period.

The State will:

- Develop, maintain and update the State IT Security Policies, including applicable State information risk policies, standards and procedures.
- Provide a State Single Point of Contact with responsibility for account security audits;
- Support intrusion detection and prevention and vulnerability scanning pursuant to State IT Security Policies;
- Provide the State security audit findings material for the Services based upon the security policies, standards and practices in effect as of the Effective Date and any subsequent updates.
- Assist the Contractor in performing a baseline inventory of access IDs for the systems for which the Contractor has security responsibility;
- Authorize User IDs and passwords for the State personnel for the Systems software, software tools and network infrastructure systems and devices under Contractor management;
- Approve non-expiring passwords and policy exception requests, as appropriate.

3.1. State Provided Elements: Contractor Responsibility Considerations

The State is responsible for Network Layer (meaning the internet Protocol suite and the open systems interconnection model of computer networking protocols and methods to process communications across the IP network) system services and functions that build upon State infrastructure environment elements, the Contractor shall not be responsible for the implementation of Security Services of these systems as these shall be retained by the State.

To the extent that Contractor's access or utilize State provided networks, the Contractor is responsible for adhering to State policies and use procedures and do so in a manner as to not diminish established State capabilities and standards.

The Contractor will be responsible for maintaining the security of information in environment elements that it accesses, utilizes, develops or manages in accordance with the State Security Policy. The Contractor will implement information security policies and capabilities, upon review and agreement by the State, based on the Contractors standard service center security processes that satisfy the State's requirements contained herein.

The Contractor's responsibilities with respect to security services must also include the following:

- Support intrusion detection & prevention including prompt agency notification of such events, reporting, monitoring and assessing security events.
- Provide vulnerability management services including supporting remediation for identified vulnerabilities as agreed.
- Support the State IT Security Policy which includes the development, maintenance, updates, and implementation of security procedures with the agency's review and approval, including physical access strategies and standards, ID approval procedures and a breach of security action plan.
- Support OIT in the implementation, maintenance and updating of statewide data security policies, including the State information risk policies, standards and procedures.
- Managing and administering access to the systems, networks, Operating Software or System Software, (including programs, device drivers, microcode and related code supporting documentation and media that: 1) perform tasks basic to the functioning of data processing and network connectivity; and 2) are required to operate Applications Software), systems files and the State Data.
- Supporting the State in implementation of programs to raise the awareness of End Users and staff personnel as to the existence and importance of security policy compliance.
- Installing and updating State provided or approved system security Software, assigning and resetting passwords per established procedures, providing the agency access to create user ID's, suspend and delete inactive logon IDs, research system security problems, maintain network access authority, assisting in processing the agency requested security requests, performing security audits to confirm that adequate security procedures are in place on an ongoing basis, with the agency's assistance providing incident investigation support, and providing environment and server security support and technical advice.
- Developing, implementing, and maintaining a set of automated and manual processes so that the State data access rules, as they are made known by the State, are not compromised.
- Performing physical security functions (e.g., identification badge controls, alarm responses) at the facilities under Contractor control.

3.2. Periodic Security and Privacy Audits

The State shall be responsible for conducting periodic security and privacy audits and generally utilizes members of the OIT Chief Information Security Officer and Privacy teams, the OBM Office of Internal Audit and the Auditor of State, depending on the focus area of an audit. Should an audit issue or finding be discovered the following resolution path shall apply:

- If a security or privacy issue is determined to be pre-existing to this agreement, the State will have responsibility to address or resolve the issue. Dependent on the nature of the issue the State may elect to contract with the Contractor under mutually agreeable terms for those specific resolution services at that time or elect to address the issue independent of the Contractor.

- For in-scope environments and services, all new systems implemented or deployed by the Contractor shall comply with State security and privacy policies.

3.3. Annual Security Plan: State and Contractor Obligations

The Contractor will develop, implement and thereafter maintain annually a Security Plan for review, comment and approval by the State Information Security and Privacy Officer, that a minimum must include and implement processes for the following items related to the system and services:

- Security policies
- Logical security controls (privacy, user access and authentication, user permissions, etc.)
- Technical security controls and security architecture (communications, hardware, data, physical access, software, operating system, encryption, etc.)
- Security processes (security assessments, risk assessments, incident response, etc.)
- Detail the technical specifics to satisfy the following:
- Network segmentation
- Perimeter security
- Application security and data sensitivity classification
- PHI and PII data elements
- Intrusion management
- Monitoring and reporting
- Host hardening
- Remote access
- Encryption
- State-wide active directory services for authentication
- Interface security
- Security test procedures
- Managing network security devices
- Security patch management
- Detailed diagrams depicting all security-related devices and subsystems and their relationships with other systems for which they provide controls
- Secure communications over the Internet

The Security Plan must detail how security will be controlled during the implementation of the System and Services and contain the following:

- High-level description of the program and projects
- Security risks and concerns
- Security roles and responsibilities
- Program and project security policies and guidelines
- Security-specific project deliverables and processes
- Security team review and approval process
- Security-Identity management and Access Control for Contractor and State joiners, movers, and leavers
- Data Protection Plan for personal/sensitive data within the projects
- Business continuity and disaster recovery plan for the projects
- Infrastructure architecture and security processes
- Application security and industry best practices for the projects

- Vulnerability and threat management plan (cyber security)

3.4. State Network Access (VPN)

Any remote access to State systems and networks, Contractor or otherwise, must employ secure data transmission protocols, including the secure sockets layer (SSL) protocol and public key authentication, signing and encryption. In addition, any remote access solution must use Secure Multipurpose Internet Mail Extensions (S/MIME) to provide encryption and non-repudiation services through digital certificates and the provided PKI. Multi-factor authentication is to be employed for users with privileged network access by leveraging the State of Ohio RSA solution.

3.5. Security and Data Protection.

All Services must also operate at the [moderate level baseline] as defined in the National Institute of Standards and Technology ("NIST") 800-53 Rev. 3 [moderate baseline requirements], be consistent with Federal Information Security Management Act ("FISMA") requirements, and offer a customizable and extendable capability based on open-standards APIs that enable integration with third party applications. Additionally, they must provide the State's systems administrators with 24x7 visibility into the services through a real-time, web-based "dashboard" capability that enables them to monitor, in real or near real time, the Services' performance against the established SLAs and promised operational parameters.

3.6. State Information Technology Policies

The Contractor is responsible for maintaining the security of information in environment elements under direct management and in accordance with State Security policies and standards. The Contractor will implement information security policies and capabilities as set forth in Statements of Work and, upon review and agreement by the State, based on the Offeror's standard service center security processes that satisfy the State's requirements contained herein. The Offeror's responsibilities with respect to security services include the following:

- Support intrusion detection & prevention including prompt agency notification of such events, reporting, monitoring and assessing security events.
- Support the State IT Security Policy which includes the development, maintenance, updates, and implementation of security procedures with the agency's review and approval, including physical access strategies and standards, ID approval procedures and a breach of security action plan.
- Managing and administering access to the Operating Software, systems files and the State Data.
- Installing and updating State provided or approved system security Software, assigning and resetting administrative passwords per established procedures, providing the agency access to create administrative user ID's, suspending and deleting inactive logon IDs, researching system security problems, maintaining network access authority, assist processing of the agency requested security requests, performing security audits to confirm that adequate security procedures are in place on an ongoing basis, with the agency's assistance providing incident investigation support, and providing environment and server security support and technical advice.
- Developing, implementing, and maintaining a set of automated and manual processes so that the State data access rules are not compromised.
- Where the Contractor identifies a potential issue in maintaining an "as provided" State infrastructure element with the more stringent requirement of an agency security policy (which may be federally mandated or otherwise required by law), identifying to agencies the nature of the issue, and if possible, potential remedies for consideration by the State agency.
- The State shall be responsible for conducting periodic security and privacy audits and generally utilizes members of the OIT Chief Information Security Officer and Privacy teams, the OBM Office of Internal Audit and the Auditor of State, depending on the focus area of an audit. Should an audit issue be discovered the following resolution path shall apply:

- If a security or privacy issue is determined to be pre-existing to this agreement, the State will have responsibility to address or resolve the issue. Dependent on the nature of the issue the State may elect to contract with the Contractor under mutually agreeable terms for those specific resolution services at that time or elect to address the issue independent of the Contractor.
- If over the course of delivering services to the State under this Statement of Work for in-scope environments the Contractor becomes aware of an issue, or a potential issue that was not detected by security and privacy teams the Contractor is to notify the State within two (2) hours. This notification shall not minimize the more stringent Service Level Agreements pertaining to security scans and breaches contained herein, which due to the nature of an active breach shall take precedence over this notification. Dependent on the nature of the issue the State may elect to contract with the Contractor under mutually agreeable terms for those specific resolution services at that time or elect to address the issue independent of the Contractor.
- For in-scope environments and services, all new systems implemented or deployed by the Contractor shall comply with State security and privacy policies.

The Contractor will comply with State Security and Privacy policies and standards. For purposes of convenience, a compendium of links to this information is provided in the Table below.

State of Ohio Security and Privacy Policies

Item	Link
Statewide IT Standards	http://das.ohio.gov/Divisions/InformationTechnology/StateofOhioITStandards.aspx
Statewide IT Bulletins	http://das.ohio.gov/Divisions/InformationTechnology/StateofOhioITBulletins.aspx
IT Policies and Standards	http://das.ohio.gov/Divisions/InformationTechnology/StateofOhioITPolicies/tabid/107/Default.aspx
DAS Policies	100-11 Protecting Privacy), (700 Series – Computing) and (2000 Series – IT Operations and Management) http://das.ohio.gov/Divisions/DirectorsOffice/EmployeesServices/DASPolicies/tabid/463/Default.aspx

4. State and Federal Data Privacy Requirements

Because the privacy of individuals' personally identifiable information (PII) and State Sensitive Information, generally information that is not subject to disclosures under Ohio Public Records law, (SSI) is a key element to maintaining the public's trust in working with the State, all systems and services shall be designed and shall function according to the following fair information practices principles. To the extent that personally identifiable information in the system is "protected health information" under the HIPAA Privacy Rule, these principles shall be implemented in alignment with the HIPAA Privacy Rule. To the extent that there is PII in the system that is not "protected health information" under HIPAA, these principles shall still be implemented and, when applicable, aligned to other law or regulation.

All parties to this agreement specifically agree to comply with state and federal confidentiality and information disclosure laws, rules and regulations applicable to work associated with this RFP including but not limited to:

- United States Code 42 USC 1320d through 1320d-8 (HIPAA);
- IRS 1075 pertaining to FTI data;
- Code of Federal Regulations, 42 CFR 431.300, 431.302, 431.305, 431.306, 435.945,45 CFR164.502 (e) and 164.504 (e);
- Ohio Revised Code, ORC 173.20, 173.22, 1347.01 through 1347.99, 2305.24, 2305.251, 3701.243, 3701.028, 4123.27, 5101.26, 5101.27, 5101.572, 5112.21, and 5111.61; and
- Corresponding Ohio Administrative Code Rules and Updates.
- Systems and Services must support and comply with the State's security operational support model which is aligned to NIST 800-53 Revision 3.

4.1. Protection of State Data

Protection of State Data. To protect State Data as described in this agreement, in addition to its other duties regarding State Data, Contractor will:

- Maintain in confidence any personally identifiable information ("PI") and State Sensitive Information ("SSI") it may obtain, maintain, process, or otherwise receive from or through the State in the course of the Agreement;
- Use and permit its employees, officers, agents, and independent contractors to use any PI/SSI received from the State solely for those purposes expressly contemplated by the Agreement;
- Not sell, rent, lease or disclose, or permit its employees, officers, agents, and independent contractors to sell, rent, lease, or disclose, any such PI/SSI to any third party, except as permitted under this Agreement or required by applicable law, regulation, or court order;
- Take all commercially reasonable steps to (a) protect the confidentiality of PI/SSI received from the State and (b) establish and maintain physical, technical and administrative safeguards to prevent unauthorized access by third parties to PI/SSI received by Contractor from the State;
- Give access to PI/SSI of the State only to those individual employees, officers, agents, and independent contractors who reasonably require access to such information in connection with the performance of Contractor's obligations under this Agreement;
- Upon request by the State, promptly destroy or return to the State in a format designated by the State all PI/SSI received from the State;
- Cooperate with any attempt by the State to monitor Contractor's compliance with the foregoing obligations as reasonably requested by the State from time to time. The State shall be responsible for all costs incurred by Contractor for compliance with this provision of this subsection;
- Establish and maintain data security policies and procedures designed to ensure the following:

a) Security and confidentiality of PI/SSI;
b) Protection against anticipated threats or hazards to the security or integrity of PI/SSI; and
c) Protection against the unauthorized access or use of PI/SSI.

4.1.1. Disclosure

Disclosure to Third Parties. This Agreement shall not be deemed to prohibit disclosures in the following cases:

- Required by applicable law, regulation, court order or subpoena; provided that, if the Contractor or any of its representatives are ordered or requested to disclose any information provided by the State, whether PI/SSI or otherwise, pursuant to court or administrative order, subpoena, summons, or other legal process, Contractor will promptly notify the State (unless prohibited from doing so by law, rule, regulation or court order) in order that the State may have the opportunity to seek a protective order or take other appropriate action. Contractor will also cooperate in the State's efforts to obtain a protective order or other reasonable assurance that confidential treatment will be accorded the information provided by the State. If, in the absence of a protective order, Contractor is compelled as a matter of law to disclose the information provided by the State, Contractor may disclose to the party compelling disclosure only the part of such information as is required by law to be disclosed (in which case, prior to such disclosure, Contractor will advise and consult with the State and its counsel as to such disclosure and the nature of wording of such disclosure) and Contractor will use commercially reasonable efforts to obtain confidential treatment therefore;
- To State auditors or regulators;
- To service providers and agents of either party as permitted by law, provided that such service providers and agents are subject to binding confidentiality obligations; or
- To the professional advisors of either party, provided that such advisors are obligated to maintain the confidentiality of the information they receive.

4.2. Handling the State's Data

The Contractor must use due diligence to ensure computer and telecommunications systems and services involved in storing, using, or transmitting State Data are secure and to protect that data from unauthorized disclosure, modification, or destruction. “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. To accomplish this, the Contractor must adhere to the following principles:

- Apply appropriate risk management techniques to balance the need for security measures against the sensitivity of the State Data.
- Ensure that its internal security policies, plans, and procedures address the basic security elements of confidentiality, integrity, and availability.
- Maintain plans and policies that include methods to protect against security and integrity threats and vulnerabilities, as well as detect and respond to those threats and vulnerabilities.
- Maintain appropriate identification and authentication processes for information systems and services associated with State Data.
- Maintain appropriate access control and authorization policies, plans, and procedures to protect system assets and other information resources associated with State Data.
- Implement and manage security audit logging on information systems, including computers and network devices.

4.3. Contractor Access to State Networks Systems and Data

The Contractor must maintain a robust boundary security capacity that incorporates generally recognized system hardening techniques. This includes determining which ports and services are required to support access to systems that hold State Data, limiting access to only these points, and disable all others.

To do this, the Contractor must:

- Use assets and techniques such as properly configured firewalls, a demilitarized zone for handling public traffic, host-to-host management, Internet protocol specification for source and destination, strong authentication, encryption, packet filtering, activity logging, and implementation of system security fixes and patches as they become available.
- Use two-factor authentication to limit access to systems that contain particularly sensitive State Data, such as personally identifiable data.
- Assume all State Data and information is both confidential and critical for State operations, and the Contractor’s security policies, plans, and procedure for the handling, storage, backup, access, and, if appropriate, destruction of that data must be commensurate to this level of sensitivity unless the State instructs the Contractor otherwise in writing.
- Employ appropriate intrusion and attack prevention and detection capabilities. Those capabilities must track unauthorized access and attempts to access the State’s Data, as well as attacks on the Contractor’s infrastructure associated with the State’s data. Further, the Contractor must monitor and appropriately address information from its system tools used to prevent and detect unauthorized access to and attacks on the infrastructure associated with the State’s Data.
- Use appropriate measures to ensure that State Data is secure before transferring control of any systems or media on which State Data is stored. The method of securing the State Data must be appropriate to the situation and may include erasure, destruction, or encryption of the State Data before transfer of control. The transfer of any such system or media must be reasonably necessary for the performance of the Contractor’s obligations under this Contract.
- Have a business continuity plan in place that the Contractor tests and updates at least annually. The plan must address procedures for response to emergencies and other business interruptions. Part of the plan must address backing up and storing data at a location sufficiently remote from the facilities at which the Contractor maintains the State’s Data in case of loss of that data at the primary site. The plan also must address the rapid restoration, relocation, or replacement of resources associated with the State’s Data in the case of a disaster or other business interruption. The Contractor’s business continuity plan must address short- and long-term restoration, relocation, or replacement of resources that will ensure the smooth continuation of operations related to the State’s Data. Such resources may include, among others,

communications, supplies, transportation, space, power and environmental controls, documentation, people, data, software, and hardware. The Contractor also must provide for reviewing, testing, and adjusting the plan on an annual basis.

- Not allow the State's Data to be loaded onto portable computing devices or portable storage components or media unless necessary to perform its obligations under this Contract properly. Even then, the Contractor may permit such only if adequate security measures are in place to ensure the integrity and security of the State Data. Those measures must include a policy on physical security for such devices to minimize the risks of theft and unauthorized access that includes a prohibition against viewing sensitive or confidential data in public or common areas.
- Ensure that portable computing devices must have anti-virus software, personal firewalls, and system password protection. In addition, the State's Data must be encrypted when stored on any portable computing or storage device or media or when transmitted from them across any data network.
- Maintain an accurate inventory of all such devices and the individuals to whom they are assigned.

4.4. Portable Devices, Data Transfer and Media

Any encryption requirement identified in this Supplement means encryption that complies with National Institute of Standards Federal Information Processing Standard 140-2 as demonstrated by a valid FIPS certificate number. Any sensitive State Data transmitted over a network, or taken off site via removable media must be encrypted pursuant to the State's Data encryption standard ITS-SEC-01 Data Encryption and Cryptography.

The Contractor must have reporting requirements for lost or stolen portable computing devices authorized for use with State Data and must report any loss or theft of such to the State in writing as quickly as reasonably possible. The Contractor also must maintain an incident response capability for all security breaches involving State Data whether involving mobile devices or media or not. The Contractor must detail this capability in a written policy that defines procedures for how the Contractor will detect, evaluate, and respond to adverse events that may indicate a breach or attempt to attack or access State Data or the infrastructure associated with State Data.

To the extent the State requires the Contractor to adhere to specific processes or procedures in addition to those set forth above in order for the Contractor to comply with the managed services principles enumerated herein, those processes or procedures are set forth in this agreement.

4.5. Limited Use; Survival of Obligations.

Contractor may use PI/SSI only as necessary for Contractor's performance under or pursuant to rights granted in this Agreement and for no other purpose. Contractor's limited right to use PI/SSI expires upon conclusion, non-renewal or termination of this Agreement for any reason. Contractor's obligations of confidentiality and non-disclosure survive termination or expiration for any reason of this Agreement.

4.6. Disposal of PI/SSI.

Upon expiration of Contractor's limited right to use PI/SSI, Contractor must return all physical embodiments to the State or, with the State's permission; Contractor may destroy PI/SSI. Upon the State's request, Contractor shall provide written certification to the State that Contractor has returned, or destroyed, all such PI/SSI in Contractor's possession.

4.7. Remedies

If Contractor or any of its representatives or agents breaches the covenants set forth in these provisions, irreparable injury may result to the State or third parties entrusting PI/SSI to the State. Therefore, the State's remedies at law may be inadequate and the State shall be entitled to seek an injunction to restrain any continuing breach. Notwithstanding any limitation on Contractor's liability, the State shall further be entitled to any other rights or remedies that it may have in law or in equity.

4.8. Prohibition on Off-Shore and Unapproved Access

The Contractor shall comply in all respects with U.S. statutes, regulations, and administrative requirements regarding its relationships with non-U.S. governmental and quasi-governmental entities including, but not limited to the export control regulations of the International Traffic in Arms Regulations ("ITAR") and the Export Administration Act ("EAA"); the anti-boycott and embargo regulations and guidelines issued under the EAA, and the regulations of the U.S. Department of the Treasury, Office of Foreign Assets Control, HIPPA Privacy Rules and other conventions as described and required in this Supplement.

The Contractor will provide resources for the work described herein with natural persons who are lawful permanent residents as defined in 8 U.S.C. 1101 (a)(20) or who are protected individuals as defined by 8 U.S.C. 1324b(a)(3). It also means any corporation, business association, partnership, society, trust, or any other entity, organization or group that is incorporated to do business in the U.S. It also includes any governmental (federal, state, local), entity.

The State specifically excludes sending, taking or making available remotely (directly or indirectly), any State information including data, software, code, intellectual property, designs and specifications, system logs, system data, personal or identifying information and related materials out of the United States in any manner, except by mere travel outside of the U.S. by a person whose personal knowledge includes technical data; or transferring registration, control, or ownership to a foreign person, whether in the U.S. or abroad, or disclosing (including oral or visual disclosure) or transferring in the United States any State article to an embassy, any agency or subdivision of a foreign government (e.g., diplomatic missions); or disclosing (including oral or visual disclosure) or transferring data to a foreign person, whether in the U.S. or abroad.

It is the responsibility of all individuals working at the State to understand and comply with the policy set forth in this document as it pertains to end-use export controls regarding State restricted information.

Where the Contractor is handling confidential employee or citizen data associated with Human Resources data, the Contractor will comply with data handling privacy requirements associated with HIPAA and as further defined by The United States Department of Health and Human Services Privacy Requirements and outlined in http://www.hhs.gov/ocr/privacysummary.pdf

It is the responsibility of all Contractor individuals working at the State to understand and comply with the policy set forth in this document as it pertains to end-use export controls regarding State restricted information.

Where the Contractor is handling confidential or sensitive State, employee, citizen or Ohio Business data associated with State data, the Contractor will comply with data handling privacy requirements associated with the data HIPAA and as further defined by The United States Department of Health and Human Services Privacy Requirements and outlined in http://www.hhs.gov/ocr/privacysummary.pdf.

4.9. Background Check of Contractor Personnel

Contractor agrees that (1) it will conduct 3rd party criminal background checks on Contractor personnel who will perform Sensitive Services (as defined below), and (2) no Ineligible Personnel will perform Sensitive Services under this Agreement. "Ineligible Personnel" means any person who (a) has been convicted at any time of any criminal offense involving dishonesty, a breach of trust, or money laundering, or who has entered into a pre-trial diversion or similar program in connection with a prosecution for such offense, (b) is named by the Office of Foreign Asset Control (OFAC) as a Specially Designated National, or (b) has been convicted of a felony.

"Sensitive Services" means those services that (i) require access to Customer/Consumer Information, (ii) relate to the State's computer networks, information systems, databases or secure facilities under circumstances that would permit modifications to such systems, or (iii) involve unsupervised access to secure facilities ("Sensitive Services").

Upon request, Contractor will provide written evidence that all of Contractor's personnel providing Sensitive Services have undergone a criminal background check and are eligible to provide Sensitive Services. In the event

that Contractor does not comply with the terms of this section, the State may, in its sole and absolute discretion, terminate this Contract immediately without further liability.

4.10. Federal Tax Information

Contract Language for General Services

4.10.1. Performance

In performance of this Contract, the Contractor agrees to comply with and assume responsibility for compliance by his or her employees with the following requirements:

1. All work will be done under the supervision of the Contractor or the Contractor's employees.
2. Any return or return information made available in any format shall be used only for the purpose of carrying out the provisions of this Contract. Information contained in such material will be treated as confidential and will not be divulged or made known in any manner to any person except as may be necessary in the performance of this Contract.
   Disclosure to anyone other than an officer or employee of the Contractor will be prohibited.
3. All returns and return information will be accounted for upon receipt and properly stored before, during, and after processing. In addition, all related output will be given the same level of protection as required for the source material.
4. The Contractor certifies that the data processed during the performance of this Contract will be completely purged from all data storage components of his or her computer facility, and no output will be retained by the Contractor at the time the work is completed. If immediate purging of all data storage components is not possible, the Contractor certifies that any IRS data remaining in any storage component will be safeguarded to prevent unauthorized disclosures.
5. Any spoilage or any intermediate hard copy printout that may result during the processing of IRS data will be given to the agency or his or her designee. When this is not possible, the Contractor will be responsible for the destruction of the spoilage or any intermediate hard copy printouts, and will provide the agency or his or her designee with a statement containing the date of destruction, description of material destroyed, and the method used.
6. All computer systems receiving, processing, storing, or transmitting Federal Tax Information must meet the requirements defined in IRS Publication 1075. To meet functional and assurance requirements, the security features of the environment must provide for the managerial, operations, and technical controls. All security features must be available and activated to protect against unauthorized use of and access to Federal Tax Information.
7. No work involving Federal Tax Information furnished under this Contract will be subcontracted without prior written approval of the IRS.
8. The Contractor will maintain a list of employees authorized access. Such list will be provided to the agency and, upon request, to the IRS reviewing office.
9. The agency will have the right to void the Contract if the Contractor fails to provide the safeguards described above.

4.10.2. Criminal/Civil Sanctions

1. Each officer or employee of any person to whom returns or return information is or may be disclosed will be notified in writing by such person that returns or return information disclosed to such officer or employee can be used only for a purpose and to the extent authorized herein, and that further disclosure of any such returns or return information for a purpose or to an extent unauthorized herein constitutes a felony punishable upon conviction by a fine of as much as $5,000 or imprisonment for as long as 5 years, or both, together with the costs of prosecution. Such person shall also notify each such officer and employee that any such unauthorized further disclosure of returns or return information may also result in an award of civil damages against the officer or employee in an amount not less than $1,000 with respect to each instance of unauthorized disclosure. These penalties are prescribed by IRCs7213 and 7431 and set forth at 26 CFR 301.6103(n)-1.

2. Each officer or employee of any person to whom returns or return information is or may be disclosed shall be notified in writing by such person that any return or return information made available in any format shall be used only for the purpose of carrying out the provisions of this Contract. Information contained in such material shall be treated as confidential and shall not be divulged or made known in any manner to any person except as may be necessary in the performance of the Contract. Inspection by or disclosure to anyone without an official need-to-know constitutes a criminal misdemeanor punishable upon conviction by a fine of as much as $1,000 or imprisonment for as long as 1 year, or both, together with the costs of prosecution. Such person shall also notify each such officer and employee that any such unauthorized inspection or disclosure of the officer or employee (United States for Federal employees) in an amount equal to the sum of the greater of $1,000 for each act of unauthorized inspection or disclosure with respect to which such defendant is found liable or the sum of the actual damages sustained by the plaintiff as a result of such unauthorized inspection or disclosure plus in the case of a willful inspection or disclosure which is the result of gross negligence, punitive damages, plus the costs of the action. These penalties are prescribed by IRC 7213A and 7431.
3. Additionally, it is incumbent upon the Contractor to inform its officers and employees of the penalties for improper disclosure imposed by the Privacy Act of 1974, 5 U.S.C. 552a. Specifically, 5 U.S.C. 552a(i)(1), which is made applicable to contractors by 5 U.S.C. 552a(m)(1), provides that any officer or employee of a contractor, who by virtue of his/her employment or official position, has possession of or access to agency records which contain individually identifiable information, the disclosure of which is prohibited by the Privacy Act or regulations established thereunder, and who knowing that disclosure of the specific material is prohibited, willfully discloses the material in any manner to any person or agency not entitled to receive it, shall be guilty of a misdemeanor and fined not more than $5,000.

4.10.3. Criminal/Civil Sanctions

The IRS and the Agency shall have the right to send its officers and employees into the offices and plants of the Contractor for inspection of the facilities and operations provided for the performance of any work under this Contract. On the basis of such inspection, specific measures may be required in cases where the contractor is found to be noncompliant with Contract safeguards

5. Contractor Responsibilities Related to Reporting of Concerns, Issues and Security/Privacy Issues

5.1. General

If over the course of the agreement a security or privacy issue arises, whether detected by the State, a State auditor or the Contractor, that was not existing within an in-scope environment or service prior to the commencement of any Contracted service associated with this agreement, the Contractor must:

- notify the State of the issue or acknowledge receipt of the issue within two (2) hours;
- within forty-eight (48) hours from the initial detection or communication of the issue from the State, present an potential exposure or issue assessment document to the State Account Representative and the State Chief Information Security Officer with a high level assessment as to resolution actions and a plan;
- within four (4) calendar days, and upon direction from the State, implement to the extent commercially reasonable measures to minimize the State's exposure to security or privacy until such time as the issue is resolved; and
- upon approval from the State implement a permanent repair to the identified issue at the Contractor's cost; and

5.2. Actual or Attempted Access or Disclosure

If the Contractor determines that there is any actual, attempted or suspected theft of, accidental disclosure of, loss of, or inability to account for any PI/SSI by Contractor or any of its subcontractors (collectively "Disclosure") and/or any unauthorized intrusions into Contractor's or any of its subcontractor's facilities or secure systems (collectively "Intrusion"), Contractor must immediately:

- Notify the State within two (2) hours of the Contractor becoming aware of the unauthorized Disclosure or Intrusion;
- Investigate and determine if an Intrusion and/or Disclosure has occurred;
- Fully cooperate with the State in estimating the effect of the Disclosure or Intrusion's effect on the State and fully cooperate to mitigate the consequences of the Disclosure or Intrusion;
- Specify corrective action to be taken; and
- Take corrective action to prevent further Disclosure and/or Intrusion.

5.3. Unapproved Disclosures and Intrusions: Contractor Responsibilities

Contractor must, as soon as is reasonably practicable, make a report to the State including details of the Disclosure and/or Intrusion and the corrective action Contractor has taken to prevent further Disclosure and/or Intrusion. Contractor must, in the case of a Disclosure cooperate fully with the State to notify the effected persons as to the fact of and the circumstances of the Disclosure of the PI/SSI. Additionally, Contractor must cooperate fully with all government regulatory agencies and/or law enforcement agencies having jurisdiction to investigate a Disclosure and/or any known or suspected criminal activity.

- Where the Contractor identifies a potential issue in maintaining an "as provided" State infrastructure element with the more stringent of an Agency level security policy (which may be Federally mandated or otherwise required by law), identifying to Agencies the nature of the issue, and if possible, potential remedies for consideration by the State agency.
- If over the course of delivering services to the State under this Statement of Work for in-scope environments the Contractor becomes aware of an issue, or a potential issue that was not detected by security and privacy teams the Contractor is to notify the State within two (2) hour. This notification shall not minimize the more stringent Service Level Agreements pertaining to security scans and breaches contained herein, which due to the nature of an active breach shall take precedence over this notification. Dependent on the nature of the issue the State may elect to contract with the Contractor under mutually agreeable terms for those specific resolution services at that time or elect to address the issue independent of the Contractor.

5.4. Security Breach Reporting and Indemnification Requirements

- In case of an actual security breach that may have compromised State Data, the Contractor must notify the State in writing of the breach within two (2) hours of the Contractor becoming aware of the breach and fully cooperate with the State to mitigate the consequences of such a breach. This includes any use or disclosure of the State data that is inconsistent with the terms of this Contract and of which the Contractor becomes aware, including but not limited to, any discovery of a use or disclosure that is not consistent with this Contract by an employee, agent, or subcontractor of the Contractor.
- The Contractor must give the State full access to the details of the breach and assist the State in making any notifications to potentially affected people and organizations that the State deems are necessary or appropriate. The Contractor must document all such incidents, including its response to them, and make that documentation available to the State on request.
- In addition to any other liability under this Contract related to the Contractor's improper disclosure of State data, and regardless of any limitation on liability of any kind in this Contract, the Contractor will be responsible for acquiring one year's identity theft protection service on behalf of any individual or entity whose personally identifiable information is compromised while it is in the Contractor's possession. Such identity theft protection must provide coverage from all three major credit reporting agencies and provide immediate notice through phone or email of attempts to access the individuals' credit history through those services.

6. Security Review Services

As part of a regular Security Review process, the Contractor will include the following reporting and services to the State:

6.1. Hardware and Software Assets

The Contractor will support the State in defining and producing specific reports for both hardware and software assets. At a minimum this should include:

- Deviations to hardware baseline
- Inventory of information types by hardware device
- Software inventory against licenses (State purchased)
- Software versions and then scans of versions against patches distributed and applied

6.2. Security Standards by Device and Access Type

The Contractor will:

- Document security standards by device type and execute regular scans against these standards to produce exception reports
- Document and implement a process for deviation from State standards

6.3. Boundary Defenses

The Contractor will:

- Work with the State to support the denial of communications to/from known malicious IP addresses*
- Ensure that the network architecture separates internal systems from DMZ and extranet systems
- Require remote login access to use two-factor authentication
- Support the State's monitoring and management of devices remotely logging into internal network
- Support the State in the configuration firewall session tracking mechanisms for addresses that access the system

6.4. Audit Log Reviews

The Contractor will:

- Work with the State to review and validate audit log settings for hardware and software
- Ensure that all systems and environments have adequate space to store logs
- Work with the State to devise and implement profiles of common events from given systems to both reduce false positives and rapidly identify active access
- Provide requirements to the State to configure operating systems to log access control events
- Design and execute bi-weekly reports to identify anomalies in system logs
- Ensure logs are written to write-only devices for all servers or a dedicated server managed by another group.

6.5. Application Software Security

The Contractor will:

- Perform configuration review of operating system, application and database settings
- Ensure software development personnel receive training in writing secure code

6.6. System Administrator Access

The Contractor will

- Inventory all administrative passwords (application, database and operating system level)
- Implement policies to change default passwords in accordance with State policies, particular following any transfer or termination of personnel (State, existing MSV or Contractor)
- Configure administrative accounts to require regular password changes
- Ensure service level accounts have cryptographically strong passwords
- Store passwords in a hashed or encrypted format
- Ensure administrative accounts are used only for administrative activities
- Implement focused auditing of administrative privileged functions
- Configure systems to log entry and alert when administrative accounts are modified
- Segregate administrator accounts based on defined roles

6.7. Account Access Privileges

The Contractor will:

- Review and disable accounts not associated with a business process
- Create daily report that includes locked out accounts, disabled accounts, etc.
- Implement process for revoking system access
- Automatically log off users after a standard period of inactivity
- Monitor account usage to determine dormant accounts
- Monitor access attempts to deactivated accounts through audit logging
- Profile typical account usage and implement or maintain profiles to ensure that Security profiles are implemented correctly and consistently

6.8. Additional Controls and Responsibilities

The Contractor will meet with the State no less frequently than annually to:

- Review, Update and Conduct Security training for personnel, based on roles
- Review the adequacy of physical and environmental controls
- Verify the encryption of sensitive data in transit
- Review access control to information based on established roles and access profiles
- Update and review system administration documentation
- Update and review system maintenance policies
- Update and Review system and integrity policies
- Revise and Implement updates to the system security program plan
- Update and Implement Risk Assessment Policies and procedures
- Update and implement incident response procedures

RFI Section III Solution Criteria – Supporting Requirements

Line of Business	Category	Brief Description	M:Mandatory O:Optional, Nice to Have
ADA Case Management	Attachments	Ability to store pdf, word, and jpeg files and all other formats related to American Disabilities Act (ADAAA) to case folders in the case management system.	M
All	Attachments	The system will allow the option to prepare and add attachments to all elements within the system	M
Asset Management	Attachments	Provide a way to attach disposal information to records. Possibly similar to the way POs are currently attached to equipment. Maintain the current retirement/disposal approval format	M
Record Management System	Attachments	The ability to add attachments to requests or pull attachments/lists from the system	M
OIS	Dashboard	One page view of graphs that represent record "quick stats" that are completely configurable, and generally based on reports.	M
Record Management System	E-Approval	The ability for an designated authority to approve items in an electronic format.	M
Asset Management	Functionality - Ad-Hoc Custom Fields	Ability to add custom fields, which are needed for the receiving, movement and salvaging of all IT equipment.	M
Asset Management	Functionality - Ad-Hoc Custom Fields	Must have the ability to create custom fields for our use, that can are searchable, reportable, printable, etc.	M
Asset Management	Functionality - Asset Management Self-Service	Need ability to search & filter on 1) Location, 2) Office, 3) Tag#, 4) Serial#, 5) Assigned To, and 6) Needs Attention.	M
Asset Management	Functionality - Asset Management Self-Service	Easy view of all assets the currently logged in user has assigned to them.	M
Asset Management	Functionality - Asset Salvaging	Current process creates a salvage form using Julian Calendar(skid identification) generated through Asset Tracker.	M
Asset Management	Functionality - Asset Salvaging	Retirement approval system, stop-gap for asset disposal.	M

Asset Management	Functionality - Bulk Data Imports	Asset data/file imports.	M
Asset Management	Functionality - Bulk Data Imports	Staging form for data/file imports for data validation.	M
Asset Management	Functionality - Bulk Data Imports	Ability to bulk input/update by various data points including the OAKS ID number	M
Warehouse Services / General Warehouse	Functionality - Check In/Out	The ability to check in and out, and relocate inventory should be provided. The ability to edit inventory counts should also be available.	M
OIS	Functionality - Data Segregation	We need to ensure that not ALL users of the same system can see everyone else's records.	M
Asset Management	Functionality - Electric Form Creation	Delivery Form created from using scanner and Asset Tracker.	O
Warehouse Services / General Warehouse	Functionality - Electric Form Creation	The ability to generate electronic forms or lists.	M
OIS	Functionality - Email Inbound / Outbound	Status updates from within the system	O
ADA Case Management	Functionality - Historical Audit Log	Ability to timestamp all actions (edits, modification, submissions, etc.) by all users	M
Space Management	Functionality - Integration	Onboarding/Off-boarding; Records - People: Quickly, efficiently input new employees and automatically grant them access to the system for maintenance requests	O
ADA Case Management	Functionality - Knowledge Management	Create a case management system within the document library that allows investigators to create interactive case folders, add documents, contain case notes and allows data inputs for status updates	M
ADA Case Management	Functionality - Knowledge Management	Ability to upload all open/current/approved ADA cases. E-records from paper records	O
ADA Case Management	Functionality - Knowledge Management	An initial drop-off documents database that accepts submitted ADA requests and all other ADA related documents electronically	M
ADA Case Management	Functionality - Knowledge Management	Ability to bank/store employee Position Descriptions necessary to ADA evaluations or a request notification function that allows for investigation to request Position Descriptions	O

ADA Case Management	Functionality - Knowledge Management	Warehouse: Warehouse database for ADA training materials	O
Maintenance	Functionality - Maps	Maintenance Request Mapping	O
Space Management	Functionality - Maps	Interactive Map of Facilities	M
Space Management	Functionality - Maps	Space Audit Functionality: Records - Space: Ability to easily walk a space and confirm employee seating locations, workstation sizes/layouts, etc.	O
ADA Case Management	Functionality - Overview Screen	Creation of a matrix/dashboard for easy view of ADA cases	O
ADA Case Management	Functionality - Overview Screen	Overview of worklist with status of workflow stage that is required for each unique BCR employee (showing only their actions); based on user security	M
Asset Management	Functionality - Overview Screen	Overview that shows all JFS assets in one screen.	M
Forms Management	Functionality - Overview Screen	Overview of worklist w/ status of workflow stage. This required on the Forms Management business side.	M
Forms Management	Functionality - Overview Screen	Overview of worklist w/ status of workflow stage. This required for each unique customer (showing only their actions); based on user security	M
ALL	Functionality - Printing	Print all data points from Asset Configuration Item (CI) on the fly (Ex: on an asset and print specific asset)	O
Asset Management	Functionality - Purchase Order Cross-Reference	A method of pulling all line items from PO, and matching specific individual lines to one single asset.	M
ALL	Functionality - Record Assignment	View & Remove Assigned User(s) & Support Group(s): View of All Previously and Currently Assigned User(s), Support Group(s), etc., as well as Removal of any Current assignment.	M
ALL	Functionality - Record Assignment	View User Details from CI: Can view all user info from CI, including (but not limited to): email, phone, location, etc..	M
ALL	Functionality - Record Assignment	View Support Group Details from CI: Can view all Support Group info from CI, including (but not limited to): Support Staff, Supervisor, Manager, mailbox, etc..	M

ADA Case Management	Functionality - Record Entry Methods	Interactive system that allows input from automatic sources (through fax and email) from all systems to determine a single point that can be viewed to determine the status of an ADA requests. Allow submissions from both internal and external sources	M
ADA Case Management	Functionality - Record Entry Methods	Interactive system that allows input from manual sources that can be viewed to determine the status of ADA requests	M
Record Management System	Functionality - Record Entry Methods	The ability to create, edit, relocate, add and purge record boxes. Adding/creating boxes should be accessible through mobile devices, scanners and tablets, also.	M
Forms Management	Functionality - Relationships	Ability to manually enter cross-reference information for a particular form.	M
Space Management	Functionality - Relationships	Asset Transfer for Move Requests (ex: ADA chair stays with worker)	O
Warehouse Services / General Warehouse	Functionality - Relationships	The option to connect inventory items with each other as a parent/child relationship should be provided.	M
OIS	Functionality - Scheduling	Schedule Activities: To keep track when something is done to a device (i.e. audit, hard drive swap, new RAM, etc.)	O
OIS	Functionality - Scheduling	Schedule Downtime: To show when an asset is down for maintenance, or in use by someone else.	O
Record Management System	Functionality - Self-Service	Status: A user should have the ability to put record boxes on hold, into destroy, pick-up, etc.	M
Asset Management	Functionality - Simplified Data Entry	Allow for single page data entry (versus multiple tabs) when manually entering assets	O
Asset Management	Functionality - Simplified Data Entry	Single view for all date input sources for asset updates (EX: manual entry, Atrium Discovery Dependency Mapping (ADDM), Bulk imports from all sources, etc.)	M
Asset Management	Functionality - Simultaneous Updates	Update end user's ability to allow for multiple updates (one piece of equipment) on a single screen instead of having to save and start over; tracking functionality	M

Asset Management	Functionality - Simultaneous Updates	Admins to have the ability to edit properties of more than one asset at the same time (Location, Type, Make, Model, etc.).	M
OIS	Functionality - SQL Queries	Use of SQL Queries: SQL Queries are used for multiple data points for the same field (i.e. one search for both Desktops & Laptops).	M
ADA Case Management	Functionality - Templates	Warehouse: Create a ADA template bank for correspondence (standard emails, letters, notices)	M
ADA Case Management	History	Historical/Legacy tab that provides a view for all old/ disapproved/no longer active ADA requests	M
Forms Management	History	Maintain multiple versions of numbered documents with actions, comments & audit trail attached to each iteration. Current, active documents.	M
Forms Management	History	Maintain multiple versions of numbered documents with actions, comments & audit trail attached to each iteration. (Historical form number assignments)	M
ADA Case Management	Interface	Must be able to interface with OAKS and Computer Aided Facility Management (CAFM) or any system that tracks employees employment status and employee moves	O
ADA Case Management	Interface	The system to have access to the JFS directory (IDV/LDAP) or Outlook Address book (or DAS' PeopleSoft) that will better facilitate correspondence	M
Asset Management	Interface	Interactive system that allows input from all systems so that there is a single point that can be viewed to determine the status of a piece of equipment. (ADDM, SCCM, printers, and any other systems that may detect tagged equipment) preferably with what the source of information is	M
Asset Management	Interface	Use program that keeps primary work address in database correct. Would want to use OAKS (PeopleSoft) data.	M

Asset Management	Interface	Record the asset's cost information, as required by your procurement system and fixed asset management system	M
Budget	Interface	Record Purchase Order Information, Interface to OAKS FIN - Supplier, beginning/ending dates of PO, amount, description, running total of invoices paid, total contract amount remaining, list of invoices paid against the PO, copy of PO, contract type (blanket order, payment card, etc.)	M
Forms Management	Interface	After approvals, must post to innerweb or internet as defined in specifications of the request. An administrative override of the workflow, to post in an emergency, must also be available.	M
General	Interface	Cloud-based solution is needed, so server management is not needed to support the application	M
General	Interface	Web based application, that is browser agnostic.	M
Record Management System	Interface	System Integration: The system should integrate with barcode scanner/other devices to allow for bulk importing/destructions.	M
Warehouse Services / General Warehouse	Interface	System Integration: The ability to connect with other various portals and inventory tracking systems, if necessary.	M
Warehouse Services / General Warehouse	Interface	System Integration: The system will be able to communicate with scanners to adequately count inventory once inventory is entered onto shelf locations. This will be very beneficial in situations where items are checked in and out of the same bin location.	M
Asset Management	Mobile	Use of any type of mobile device (smart phone or tablet; Apple or Android; etc.) to read a barcode to: 1) Search for an existing asset to modify, or 2) Add a new (non existing) asset entry.	O
General	Mobile	Mobile Functionality	O

Record Management System	Mobile	Entire system should be accessible via mobile device.	M
Warehouse Services / General Warehouse	Mobile	The system should be accessible on mobile devices.	M
ADA Case Management	Notification	Ability to send notifications to staff when initial ADA requests are submitted	M
ADA Case Management	Notification	Provide a notification/reminder function that automatically sends notifications to EEO staff that informs them of ADA cases that have been dormant for a fix period of time	O
ADA Case Management	Notification	Automatic notifications on all ADA status changes	O
ADA Case Management	Notification	Notification function that informs OEBS' wellness when an ergonomic evaluation is requests; in addition with the ability to preload the necessary information within the form so Wellness can fulfill the request	O
ADA Case Management	Notification	Notification function that informs OEBS' wellness of an IME; in addition with the ability to preload the necessary information within the form so Wellness can fulfill the request	O
ADA Case Management	Notification	Notification emails that can be sent automatically from the system to users	M
ADA Case Management	Notification	Ability to interactively communication through email within the interactive system with internal and external users; Possibly allowing the system to interact with Microsoft Outlook to communicate through email directly from the system	O
Budget	Notification	Record Purchase Order Information - "Notify limit" function to warn when a PO's balance is approaching a certain/set amount; Notify function to show if a PO mod has been done and the changed amount	O
Forms Management	Notification	Email and dashboard notifications for actions	M
Warehouse Services/Forms Warehouse	Notification	E-mails should be sent out automatically from the system to users.	M

Warehouse Services/Forms Warehouse	Notification	The system will recognize and notify when there is a low level of forms warehoused and create an IRN request.	M
ADA Case Management	Reporting	Must be able to produce various reports based on information submitted through inputted data	M
ADA Case Management	Reporting	Creation of filters for all data fields	M
Asset Management	Reporting	Report on progress-to-date for specific hardware replacement projects.	M
Asset Management	Reporting	Report on hardware depreciation lifecycles	M
Asset Management	Reporting	Configurable business rules to enable organizations to compare what has been discovered against what is recorded	M
Asset Management	Reporting	Must be able to produce various reports based on database tables/information sources	M
Asset Management	Reporting	Provide a report on equipment that has been dormant for a specified period of time	O
Asset Management	Reporting	Inventory Control Coordinator (ICC), or any non-IT staff, can run reports.	M
Asset Management	Reporting	Drill down by Office.	M
Asset Management	Reporting	Can track asset location, in addition to user location.	M
Asset Management	Reporting	Can view assets signed by whomever is logged in	M
Asset Management	Reporting	Historical/Legacy data tab.	M
Asset Management	Reporting	All fields reportable.	M
Asset Management	Reporting	Notifications of any changes to assets, sent to whomever is assigned to said asset(s).	M
Asset Management	Reporting	Notification Audits.	M
Asset Management	Reporting	Relationships that show different types of needs (Used by, Managed by, Owned by, etc.)?	O
Forms Management	Reporting	Ability to identify metrics & create ad-hoc reports based on various information entered for each document.	M

General	Reporting	Various System Reporting Needs - Occupancy, outstanding work tasks, submitted maintenance/move requests, employees with qualifications, asset tracking, invoice problem resolution, etc. The ability to create reports from any information listed in the system.	M
General	Reporting	Customer Service Surveys - Customer service surveys, name, comments, score	O
General	Reporting	Budget Reporting - Ability to create reports and pull information based on all of the aforementioned budgeting aspects of the system	M
Record Management System	Reporting	The ability to run reports based off records in the system including exporting reports.	M
Warehouse Services / General Warehouse	Reporting	Reporting available for all items. The ability to export reports is also a requirement.	M
Warehouse Services / Forms Warehouse	Reporting	Vendor Orders: The ability to differentiate and prepare orders for a vendor warehouse is required.	M
Asset Management	Scanners	Allow for direct input of data from barcode readers	M
Asset Management	Scanners	Asset system must be able to interface with other readers (RFID)	M
Asset Management	Scanners	Ability to apply applications to asset management functions	M
Forms Management	Scanners	Ability to use various scanning devices to track forms and interact with system to maintain stock and ordering information	M
Record Management System	Scanners	Scan guns - must be able to connect to the system to make edits and changes in location.	M
ADA Case Management	Search	Ability to search various data points (employee name, tracking number, etc.)/All fields should be searchable and reportable, sorting/filter options will be available for all fields	M
Asset Management	Search	Anyone who is not an admin, but has access to view data, can search & run reports, but NOT edit any data/fields.	M
Asset Management	Search	All fields searchable	M

Asset Management	Search	Ability to search on various data points including the OAKS ID number	M
Asset Management	Search	PO lookup via an asset, vice versa. As well as view all pertinent information that is contained in said PO (individual line items, procurement vendor, etc.). PO DETAILS	M
Record Management System	Search	All fields should be searchable and reportable. Should be able to sort, filter, etc.	M
Warehouse Services / General Warehouse	Search	All fields should be searchable and reportable. Sorting/Filter options will be available for all fields.	M
ADA Case Management	Security	Must be able to restrict access and control access to BCR staff to protect sensitive information.	M
ADA Case Management	Security	Administrative ability to roll back assignments and selections to a prior state in the workflow	M
All	Security	Control users varying level of authority and security. Ability to add/subtract/manipulate authorization level	M
All	Security	Ability to incorporate varying user roles and add employees into each category of program access.	M
All	Security	System must provide for multiple security access levels. A minimum of 5 authorization levels is required.	M
Asset Management	Security	Need to be able to add new Manufacturers, Models, etc.	M
Asset Management	Security	Ability to assign an asset to someone or a Support Group.	M
ALL	Self Service - Customer Request Portal	End users w/o any special right(s)/permission(s) can view/search/edit specific data points for Tagged CIs.	M
Forms Management	Self Service - Customer Request Portal	JFS user must initiate request with an attachment; multiple review/approval/rejection stages with ability to comment at each stage. An administrative override of the workflow to post in an emergency must also be available. (with workflow)	M

Maintenance	Self Service - Customer Request Portal	Maintenance Request Functionality; Maintenance Requests - Type, request details (who, what, when, why), description, notes, responsible person/company, resources, notes/comments, photos	M
Record Management System	Self Service - Customer Request Portal	Customers should have the ability to enter requests into the system.	M
Space Management	Self Service - Customer Request Portal	Move Request Functionality	M
Warehouse Services/Forms Warehouse	Self Service - Customer Request Portal	Internal to IM and external customers non-JFS will be able to place requests. Customers will be distinguishable by a unique ID.	M
State of Ohio	Single Sign-on	Refer to RFI attachment, "Identity Access Management"	M
State of Ohio	State Standards	Refer to RFI attachment, "Supplement Two:"	M
ALL	Ticketing	The Ticketing functionality should register an event or a ticket, assign an owner, or person responsible to the ticket, assign additional interested parties to the ticket, track changes to the ticket, inform interested parties of these changes, launch activity based on ticket status and/or priority, report on status, close the ticket.	M
ADA Case Management	Tracking	Record furniture for assigned ADA information, model, serial number, specs, manufacturer	O
ADA Case Management	Tracking	Ability to track ADA cases chronologically, by tracking number, office, date, investigator, etc.	M
ADA Case Management	Tracking	Ability to show different types of identifiers (used by, managed by, etc.)	M
ADA Case Management	Tracking	Ability to input initial data files (tracking number and type of document) that forwards the document into the main database.	M
ADA Case Management	Tracking	Ability to input/update all data points (Date rec'd, all information recorded on ADA forms, notes/comments, etc.)	M
Asset Management	Tracking	Ability to add field(s) to a CI, to keep track of something unique to no other asset in the CMDB.	O

Asset Management	Tracking	Ability to add field(s) to all Assets (CIs) , to keep track of something for all assets in the Configuration Management Data Base (CMDB).	O
Asset Management	Tracking	Easy view of all assets that have been signed for, by the currently logged in user.	M
Space Management	Tracking	Asset Tracking	O
Warehouse Services / General Warehouse	Tracking	Warehouse inventory will be tracked.	M
ALL	Tracking	For use of any verbose update that is needed. Should also be able to view previous updates and report on them.	M
ALL	Tracking	As part of the shipping/receiving process, assets are assigned to a User or Support Group on the fly.	M
Asset Management	Tracking	Track depreciation on fixed assets	M
Asset Management	Tracking	Record the asset's physical information, e.g. model, serial number, specs, manufacturer	M
Asset Management	Tracking	Used to reference what a device looks like (a picture), so it can be easily identified for pickup. This can also be used by EBS shipping/receiving group, to ensure they have the right device.	M
Asset Management	Tracking	Ability to flag/highlight verification for assets that are still in need of yearly verification.	M
Budget	Tracking	Invoices - Invoice name, description, choose contract (PO) to pay against, supplier name, invoice total to pay against PO, copy of invoice	O
Budget	Tracking	Payment Card - Works like Record PO Information and Invoices - a PO is created but the contract type is "paycard," which is then entered like an invoice	M
Budget	Tracking	Lease Information - Property address, lease type, base lease rate, commencement date, lessor contact information (legal name, billing address, contract name and number), square feet, comments section, attach documents capability	M

Budget	Tracking	Lease Information - Photo of facility	O
Budget	Tracking	Owned Property Agreements - Format to capture property address and building information (date built, square feet, etc.) on state-owned facilities	M
Budget	Tracking	Owned Property Agreements - Separate place to capture all capital improvement information as well as non-capital project information (dates, suppliers, scope of work, costs, change orders, meeting minutes, copies of purchase orders, etc.), picture of facility	M
OIS	Tracking	Ability to create and assign a contract (support, maintenance, etc.), view & remove previously assigned contracts.	M
OIS	Tracking	Add, View, Remove Relationship(s) to any and all other IT Service and Support Management (ITSSM) items, such as (but not limited to): other CIs, Tickets, etc.	O
Record Management System	Tracking	Ability to keep record retention schedules in the system in the format of a database. Currently, the list is on the Innerweb. When referencing a retention schedule in the system, ideally, the retention schedule itself would be available rather than just being reference by name.	O
Space Management	Tracking	Occupancy/Vacancy: Records - Space: Space name, description, classification, occupancy/capacity, allocation, map/graphic	M
Space Management	Tracking	General Organization/People Record Information. Records-Organization: Organization name, employees within that organization, company/external company	M
Space Management	Tracking	General People Record Information; Records - People Name, external vs internal contact, date of hire, OAKS ID, position number, organization, contact information, seat location, secondary locations, qualifications (ADA, BWC, Floor Warden, etc.)	M

Space Management	Tracking	Organization Tracking (Office, Bureau, Section); Records-Organization: Assigned color for each different office/organization	O
Space Management	Tracking	General People Record Information - Records - People: Title, appointment type (permanent/intermittent), reports to, assets, history (move log), comments and document attachments	O
Space Management (Real Estate)	Tracking	Building Information: Records - Building: Building name, address, important contacts, lease information, map/graphic, measurements (sq. ft.)	M
ADA Case Management	Tracking - History & Archive	An accessible transaction history to identify ADA equipment (person, assignment, office, location, date, etc.) or access to Facilities' interactive system that tracks ADA equipment	M
Asset Management	Tracking - History & Archive	An easily accessible transaction history for a piece of equipment. (Something similar to what is available in Tracker) person, location, date, etc.; ALL FIELDS and FUNCTIONALITY/RELATIONSHIP	M
Asset Management	Tracking - History & Archive	To reduce the volume of units in the main data files and simplify the ability to properly follow records retention schedules.	M
Asset Management	Tracking - History & Archive	Method to archive records and assets (after being disposed, EOL, etc.), so they don't show up in reports, not in user's assigned assets, etc.	M
Forms Management	Tracking - History & Archive	Maintain audit information for each change after original submission.	M
Forms Management	Tracking - History & Archive	Ability to see warehoused forms and revision dates; communicate low-level of inventory & its approval to replenish.	M
Record Management System	Tracking - History & Archive	An audit trail is necessary for all user actions.	M
Warehouse Services / General Warehouse	Tracking - History & Archive	The history details should be kept/archived for review after shipments are made.	M
Warehouse Services / General Warehouse	Tracking - History & Archive	A system user's changes, edits and actions will be tracked.	M

ADA Case Management	Workflow	Allow special allowances for EEO Manager to interactively assign/route ADA submissions to specific investigators	M
ADA Case Management	Workflow	The system will follow a standard workflow in regard to all procedures	M
ADA Case Management	Workflow	Allow multiple review/approval/rejection stages with the ability to comment at each stage. An administrative override function of the workflow should be granted in emergency and corrective situations	M
Forms Management	Workflow	Administrative ability to roll back an unpublished approval to a prior state in the workflow.	M
Record Management System	Workflow	A workflow should be followed from request to competition in all procedures.	M
Warehouse Services / General Warehouse	Workflow	The system will follow a standard workflow in regard to all procedures.	M