JFS-DAS Security Supplement Addendum

In accordance with the Governor DeWine's executive order 2019-15D:

https://governor.ohio.gov/wps/portal/gov/governor/media/executive-orders/2019-15d

ODJFS is required to participate in the InnovateOhio Platform.

IOP - Identity & Access Management

The InnovateOhio Platform (IOP) provides 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 *Application or Service* must, for all State/County employees, Businesses (Providers), and Citizens, provide single sign-on capabilities through integration with the State's Enterprise Identity Management system called Innovate Ohio Platform (IOP) leveraging IBM's Identity Federation.

IOP 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

Required Interfaces with IOP:

For all Applications and Services that require authentication and/or authorizations:

Federated Single Sign-on: Application must support federated single sign-on using SAML 2.0 OR using Open ID Connect (OIDC) for identity assertion to authenticate the user to the Application

Authorization-Based Assertion Attributes: Application, optionally but preferred, would support Token assertions to determine appropriate authorizations (roles/permissions) for the individual, upon sign-in, based upon supplied Group membership attribute(s) (or other attributes as needed).

Automation of Provisioning / de-provisioning: Application, optionally but preferred, must support either:

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

Provisioning Tasks available:

- Create, or associate, an identity in the application for authentication and single sign-on (e.g. Just in Time provisioning or achieved through Group to role inspection above).
- Assign and Change an identity's assignment to specific Roles/Permissions within the application for authorization (or achieved through Group to role inspection above).

De-provisioning Tasks available:

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

Device Authentication: Tracking device information (IP Address, OS, etc.) is required by the application. Application, optionally but preferred, would support device authentication in conjuncture with the IOP Framework above. This will support the ability to prompt for additional security validation /authentication to user in the event the device is not recognized. Such as prompting for two-factor authentication, or having the user submit to ID Proofing, or challenge response questions for additional identity validation. Once the device is identified and tied to User identity, these questions can optionally not be presented or can periodically be reaffirmed based on business requirements.

IOP – Data Analytics

All Applications must make data available to the InnovateOhio Platform for secure, resilient Data Storage, reporting, analytics and data sharing across all Cabinet Agencies, Boards, and Commissions.

In summary, ODJFS is to: (1) Make data available to the InnovateOhio Platform for storage (staging before sharing) upon request of InnovateOhio; and (2) Share data pursuant to ORC 125.32 and at the direction of InnovateOhio, acknowledging any Federal restrictions or privacy requirements.

A standing Data Sharing Protocol outlines procedures and responsibilities of DAS and agencies for use of the InnovateOhio Platform under authority of ORC 125.32 and Executive Order 2019-15D.

DAS manages the InnovateOhio Platform which consists of a set of advanced data and analytics computing technologies including a robust data governance, security and privacy protection foundation to enable usage of state data and to protect data maintained on the platform. Note that a distinction must be made between 1) an agency providing and hosting data on the platform and 2) an agency approving the use of data for analysis. When an agency provides and hosts data on the InnovateOhio Platform, the agency is not granting “use” of the data to any party including DAS. DAS’s responsibility is to manage the platform as described within this protocol under and pursuant to ORC 125.18 and ORC 125.32. DAS is not given permission to “use” agency data unless the owning agency specifically approves.

ORC 125.32 states that, “A state agency that provides data under the program retains ownership over the data. Notwithstanding any other provision of the Revised Code, only the state agency that provides data under the program may be required under the law of this state to respond to requests for records or information regarding the provided data, including public records requests, subpoenas, warrants, and investigatory requests.”

Encryption

Personally identifiable information (PII), or confidential personal information (CPI - as defined in Ohio Revised Code 1347), as used in information security and privacy laws, is information that can be used on its own or with other information to identify, contact, or locate a single person, or to identify an individual in context. One of the key security controls to protecting PII/CPI is Encryption. Encryption is to be utilized for PII/CPI data on all three states of existence:

Data at Rest: Data at Rest refers to inactive data which is stored physically in any digital form. This refers to both Structured (databases) and unstructured Data (files).

PII/CPI Data at Rest must be protected in one of the following methods:

- Encrypt the Entire Database with Transparent Data Encryption (TDE)
- Table/ Column or Field Level Encryption can be used within the Database Tables to encrypt just the PII/CPI

Ensure that any temporary representations (temp files or folders/ exports/ backups / reports, etc.) of PII/CPI is encrypted in that current state.

- Applying newer encryption technologies and techniques, such as "homomorphic encryption" can be used to meet this requirement.

Encryption methods must use compliant NIST FIPS 140-2 Encryption Algorithms.

Data in Motion: Data in Motion refers to data which is being transferred across some network or transmission media.

PII/CPI Data in Motion must be protected in one of the following methods:

- Encrypt the Entire transmission using HTTPS or IPSEC (or equivalent protocols) between all devices and tiers (such as UI > APP > DB Tiers)
- Encrypt the PII/CPI data only in transmission (Example: SOAP message using WS-Security)

Encryption methods must use compliant NIST FIPS 140-2 Encryption Algorithms / Modules. When using the Transport Layer Security (TLS), TLS version 1.2 or higher must be used.

Data in Use: Data in Use refers to data actively being used across the network or temporarily residing in memory, or any data not currently "inactive".

PII/CPI Data in Use must be protected in the following methods:

- Implement Memory protections, at a minimum, of Data Execution Prevention (DEP) and Address Space Layout Randomization (ASLR) within Hardware and/or Software.
- Sessions must be unique to each authenticated user and be protected in way that meets the Open Web Application Security Project (OWASP)'s Application Security Verification Standard (ASVS).
- Application will use per user or session indirect object references where possible. All direct object References, from an untrusted source, must include an access control check to ensure the user is authorized for the requested object.
- Ensure that authentication /authorization checks are performed at each object at the controller and business logic levels, and not just at the presentation layer.
- Prevent Injection attacks by using a parameterized API or escape special characters using the specific escape syntax for that interpreter. Also, in addition, positive or "white list" input validation must be used.
- Device configurations must confirm to industry best practices for hardening (CIS Benchmarks).
- Components, such as libraries, frameworks, or other software modules used in development must be identified and a list provided to ODJFS at the conclusion of the project. A supported version of these components must be used at time of the contract.
- Autocomplete must be disabled on forms collecting PII/CPI, and caching must be disabled for pages that contain PII/CPI.
- Avoid the use of redirects and forwards as much as possible. When used, any such destination parameters must be a mapped value, and that server-side code translates this mapping to the target URL.

Audit Logging

A log is a record of the events occurring within an organization's systems and networks. Logs are composed of log entries; each entry contains information related to a specific event that has occurred within a system or network. Many logs within an organization contain records related to computer security. These computer security logs are generated by many sources, including security software, such as antivirus software, firewalls, and intrusion detection and prevention systems; operating systems on servers, workstations, and networking equipment; and applications.

The number, volume, and variety of computer security logs have increased greatly, which has created the need for computer security log management—the process for generating, transmitting, storing, analyzing, and disposing of computer security log data. Log management is essential to ensuring that computer security records are stored in sufficient detail for an appropriate period of time. Routine log analysis is beneficial for identifying security incidents, policy violations, fraudulent activity, and operational problems. Logs are also useful when performing auditing and forensic analysis, supporting internal investigations, establishing baselines, and identifying operational trends and long-term problems. (Source NIST SP 800-92 "Guide to Computer Security Log Management")

ODJFS is required, for compliance to Federal and State Laws, codes, standards, and guidelines, to perform audit logging and management of those logs for its information systems.

Logging Requirements

The following Application Events must be record in the audit log(s) for the Information System.

Required Audit Events:

1. User account management activities (user creation, deletion, modification),
2. Application shutdown,
3. Application restart,
4. Application errors,
5. Failed and successful log-on(s),
6. Security policy modifications,
7. Use of administrator privileges,
8. All changes to logical access control authorities (e.g., rights, permissions, role assignment),
9. All system changes with the potential to compromise the integrity of audit policy configurations, security policy configurations and audit record generation services,
10. Access to Personally Identifiable Information (PII – Also known as Confidential Personal Information (CPI) by Ohio Law),
11. Modification to Personally Identifiable Information (PII) - Also known as Confidential Personal Information (CPI)by Ohio Law),
12. File creation, deletion, or modification by the application (PDF, CSV, etc. - if Applicable).

Minimum Logging Requirements for Each Event

The following are the minimum required details that must be captured with each recorded event:

1. Identity of any user/subjects associated with the event (Who – user/group/device/system),
2. Event Information (What happened),
3. What Time the event occurred (When),
4. Subsystem or application the event occurred in (Where),
5. And the success/failure of the event (if applicable).

Audit Record Generation Services

All Applications, in the event of audit log processing failure (the application is unable to write to the security log/ log service) shall:

1. Notify appropriate personnel of the audit log processing failure, and
2. shall either:
   a. Stop all processing of further request s until the audit log processing is restored, or
   b. Queue all audit events to disk, until such time as the audit log processing is restored or the storage allocation is filled.

If storage allocation is full, the application shall stop all processing of all further requests until the audit log processing is restored.

Audit Retention, Aggregation, and Analysis

Applications are required to send the Audit Event Log information, through standard processes (such as SYSLOG) or through add-ons, to the Agencies Enterprise Log Management (ELM) Tool – Splunk and Enterprise Security Information and Event Management (SIEM) – QRadar.

Any required third-party tools or services to achieve this requirement, the vendor must acquire, purchase, and setup.

Audit Log information must be sent security to ODJFS ELM and/or SIEM tools and CPI Log repository (when applicable), using encryption methods that use compliant NIST FIPS 140-2 Encryption Algorithms / Modules.

Development Security

Data Set used in Development

All Data sets used in non-production environments (Development, Quality Testing, User Acceptance testing, etc.) must be generated or masked data or data sets (not real production data). Except, where approved by Agency Security Official, and using the same set of security controls that are in place for the non-production environment as the production environment. Masked or generated data or data sets can be generated by ODJFS for these purposes.

DevOps Vulnerability Scanning

Applications being developed for hosting by the state (on-premise) must adhere to ODJFS DevOps pipeline AppSec tools and processes. This includes both Static (code or white-box scanning) and Dynamic (application or black-box scanning) vulnerability scanning. Additionally,

any libraries or components used in the solution must be free of known critical or severe vulnerabilities and be scanned/evaluated by the ODJFS Software Composition Analysis (SCA) tool.

Hosted Solutions or Software as a Service (SaaS) Applications or Services. The vendor must provide proof that these scans are being performed and evaluated internally as part of their SDLC/DevOps processes, or by third Party compliance assessment certification/attestation (FedRAMP, ISO 27001, OWASP ASVS, CSA STAR, etc.).