FLORIDA DEPARTMENT OF JUVENILE JUSTICE

October 15, 2024

The Honorable Doug Broxson
Chair, Senate Appropriations Committee
201 The Capitol
404 South Monroe Street
Tallahassee, FL 32399-1100

The Honorable Tom Leek
Chair, House Appropriations Committee
221 The Capitol
402 South Monroe Street
Tallahassee, FL 32399-1300

Mr. Daniel Pardo and Ms. Brandi Gunder
Office of Policy & Budget
PL 05 The Capitol
Tallahassee, FL 32399-0001

Dear Chair Broxson, Chair Leek, Mr. Pardo, and Ms. Gunder:

In accordance with section 282.206, Florida Statues, please find below the Department of Juvenile Justice's Cloud First Strategic Policy Report. Should you have any questions, please do not hesitate to contact me or our staff.

Sincerely,

Eric S. Hall
Secretary

The Florida Department of Juvenile Justice Cloud First Strategic Plan 2024

1) Executive Summary

The Bureau of Information Technology (IT) must deliver accurate and timely information to ensure the organization is able to realize positive strategic, financial and operational outcomes. Regardless of the assigned program area or geographical location, each agency user must be able to access, process, and analyze information for operational continuity purposes. As part of these efforts, this includes considering cloud hardware and software solutions as they relate to new or existing technologies. The Bureau of Information Technology's primary purpose for defining this strategy is to ensure proper alignment of the implementation of cloud services with DJJ IT's goals, policies and related regulatory requirements.

2) Objective

This plan establishes guidelines for evaluating all agency software and hardware solutions for cloud feasibility while enforcing compliance with required security policies, procedures, and standards. The Department of Juvenile Justice (DJJ) shall monitor, control, and protect data, network infrastructure and IT resources by using secure software development and system engineering principles. Private cloud infrastructure services will remain components in DJJ's long-term cloud strategy.

The desired outcome of the strategy and recommendations proposed within this document is to transition the Department away from the business of data center management. Migration to cloud-based services supports IT's core value, vision and mission statements by embracing innovative technology solutions and the agility of cloud computing.

3) Current Situation

a. *Environment*: DJJ's network environment operates exclusively on a Microsoft platform and currently consists of approximately 1208 workstations, 600 laptops, 2009 Tablets, 267 Printers and 145 servers. These servers include domain controllers, SQL database servers, Internet/Intranet servers, data servers and print servers.

b. *Applications*: The Juvenile Justice Information System (JJIS) is a statewide case management system that collects data on a juvenile from the time they enter the DJJ system until they leave the custody of the DJJ. JJIS has twenty-two internal business applications developed using .NET and Microsoft SQL Databases which supports the core business function. JJIS was implemented in 1998 and is used by approximately 9,087 users to include DJJ employees, providers, court staff, state agencies and law enforcement partners. JJIS contains approximately 1.65 million youth records, over 4.7 million referral and medical records, and uses more than 5.89 TB of disk space. JJIS provides data for evaluating juvenile trends,

programs and reports used to manage the effectiveness and efficiency of the Department's processes and procedures.

c. *Staffing and Budget*: IT currently has 60.5 FTE and 13 contracted positions to support over 3,200 department users and approximately 120 different providers with over 2,500 staffs within an annual operating budget of approximately 10.93 million dollars.
d. *System Users:* DJJ currently has approximately 6,000 network users.
e. *Important Interfaces*: DJJ currently shares data with many Criminal Justice entities and a few non-Criminal Justice entities. JJIS currently shares data with the Florida Department of Law Enforcement (FDLE), Florida Department of Highway Safety, Florida Department of Children and Families, Florida Department of Education, Florida Courts, and multiple law enforcement entities located outside of state agencies. JJIS data is shared with authorized users using multiple mechanisms such as CJNET, nightly data uploads, and standardized web services. All data sharing utilizes a data sharing agreement to ensure integrity and compliance with agency policy and procedures.

4) Transition

a. *Architectural Overview*: Except for Office 365 products, both web servers (Internet & Intranet), and Axiom-Pro server (A digital imaging system), all other agency applications are housed on local servers in the Florida Department of Management Services, or Northwest Regional Data Center (NWRDC).
b. *Transition*: The first step of the process was to establish Active Directory (AD) in the cloud. As part of this process, seven servers were established in Azure. Two AD servers, two Active Directory Federation Services (ADFS)* servers, two proxy servers and one ADCONNECT server. To accomplish this, DJJ, approved by FDLE under CJIS policy, entered into a contractual agreement with the Northwest Regional Data Center (NWRDC) for Azure (Cloud) services. This first step was completed in October 2020.

   The Agency has since requested and obtained permission and have established an Enterprise Agreement (EA) directly with Microsoft. Azure assessment test on servers to determine viability on migration was completed January 2023.

   Express Route connection to Microsoft Network has been established.

DJJ is moving.

IT is migrating in phases. Migration of the test servers is complete, and migration of the development servers is underway. The production servers will be the last to migrate and our plan is to be fully in the cloud by fiscal year 2025/2026.

DJJ has moved away from Cisco virtual appliances in Azure. We are using Office 365 mail gateway as replacement for Cisco ESA and Zscaler to replace Cisco WSA as the Web Proxy.

The agency completed the migration of the current Internet/Intranet software to a cloud environment.

*Active Directory Federation Services is a software component that provide users with single sign-on access to systems and applications located across organizational boundaries.

c. *Approach*: The Department will examine cloud availability options to ensure continuity of business operations. At minimum, the below must be considered:

i. Security

1. All Criminal Justice Information System (CJIS) Computer Security Policy requirements MUST always be satisfied and maintained.
2. The Type of Data (e.g., CJIS versus non-CJIS) to be stored must be considered as this will help select appropriate cloud storage, prevent exposure over IPs, enforce least privilege using object versioning, create immutable backups with recovery plans, enable encryption, and regularly review data security measures.
3. How will the cloud application be accessed? Are there measures in place to log who is accessing data and what data is being accessed?
4. Cloud resources must implement controls in their tenant to prevent and detect MCA (Malicious Cyber Actors). Zero Trust network security practices, such as evaluating identity information in all requests, micro segmentation, and end-to-end encryption should be used to protect organizational data.
5. Stability of Cloud Provider must be considered when evaluating solutions to ensure continuity, reliability, and operational support that's conducive to our environment and our long-term success. This includes certifications and standards, policies on data governance and security, reputations for reliability, key technologies used, and partnerships and service dependencies.

ii. Operational

1. Services Provided: It is important to determine exactly what services are needed, who are the stakeholders, are the performance metrics defined in the Service Level Agreement (SLA) acceptable, how will these metrics be monitored by the agency, and what financial consequences are imposed when the vendor does not meet the minimum standards of the SLA?
2. Organization Bandwidth. This must be considered as this is the connectivity to the cloud solutions. If connectivity speeds are not optimal, the full benefits of the cloud solution(s) are not realized.
3. System/Application limitations. In some cases, and for a variety of reasons, it is not feasible to migrate an application from an on-premises solution to the cloud. If any of these limitations can be mitigated, the time and associated costs to do so must be considered when evaluating a potential cloud solution.
4. Disaster Recovery. In the event of a disaster, how long will it take to restore full system operations? What about the restoration of files? This should be specifically addressed in the SLA between DJJ and the cloud provider.

iii. Contractual

1. Budget. Most cloud solutions are subscription based, so accounting for recurring costs, which include accounting for growth over a period of time, must be considered. This includes any additional positions which may be needed to maintain new functionality.
2. Exit strategy. If the company providing the cloud solution in question dissolves or their services are no longer needed, what happens to the data?