

The Florida Department of Juvenile Justice Cloud First Strategic Plan 2023

1) Executive Summary

The Bureau of Information Technology (IT) must deliver accurate and timely information to ensure the organization is able to always make cost effective and highly knowledgeable business decisions. Regardless of the assigned program area or geographical location, each agency user must be able to access, process, and analyze needed 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.

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.

3) Current Situation

- a. *Environment.* DJJ's network environment operates exclusively on a Microsoft platform and currently consists of approximately 2579 workstations, 299 laptops, 1542 Tablets and 145 servers. These servers include domain controllers, SQL database servers, Internet/Intranet servers, data servers and print servers.
- b. *Applications:* DJJ currently has 22 internal business applications. These applications were developed using .NET and Microsoft SQL Databases. The core business application for the agency is the Juvenile Justice Information System (JJIS). This application is used throughout all program areas for case management purposes to track all youth in the system from the point of entry until all requirements have been met, or the youth ages out of the system. JJIS was implemented in 1998, contains approximately 1.65 million youth records, over 4.6 million referral records, and uses more than 5.5 TB of disk space. JJIS is used by approximately 7,150 users which include DJJ employees, DJJ contracted providers, and agency partners (e.g., Law Enforcement).
- c. *Staffing and Budget.* The Bureau of Information Technology currently has 60.5 FTE and 13 contracted positions to support over 3,200 organization users and approximately 120 different providers within an annual operating budget of approximately 9.05 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

The Florida Department of Juvenile Justice Cloud First Strategic Plan 2023

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 currently housed on local servers located in the Florida Department of Management Services, or Northwest Regional (NWRDC) Data Center.
- b. *Transition:* As part of the transition to the cloud, DJJ has started the migration process to Azure cloud.

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.

The department is ready to migrate and will be moving in phases. IT will migrate test servers first, after testing and acceptance we will move the development servers and lastly the production servers. We plan to be fully in the cloud by fiscal year 2024/2025.

Additionally, DJJ is planning to establish two Cisco virtual appliances in Azure when the time comes to renew the contract for the replacement of on-premises appliances. It is much more cost effective to move to the virtual appliances. These appliances will be used for the organization web filter (Cisco WSA) and email gateway (Cisco ESA), respectively.

The agency has 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.

The Florida Department of Juvenile Justice Cloud First Strategic Plan 2023

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 determine which cloud options are viable.
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. Stability of Cloud Provider must be considered when evaluating solutions to ensure continuity, reliability, and operational support.

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?