2024

Florida Fish and Wildlife Conservation Commission Cloud First Strategic Plan

Submitted on:

October 15, 2024

Table of Contents

Executive Summary

Florida Fish and Wildlife Conservation Commission (FWC) completed its efforts to migrate applications from the State Data Center to the cloud. This correlated with adopting a cloud-first policy focused on utilizing cloud-computing solutions that minimize or do not require using the state data center infrastructure when applicable. FWC successfully migrated all systems and services to the cloud and no longer has servers in the state data center.

Cloud migrations have provided many benefits, including:

- Backups—FWC has direct access to create and maintain backup retention policies and retain snapshots of servers on a rotational daily basis. Restores are timely and easily accessible to the customer.

- Disaster Recovery / Failover—FWC can use the utility built into Microsoft Azure with preconfigured routing and bandwidth allocations to respond quickly to outages. This can be used for the entire cloud environment.

- Resilient—Migration to the cloud provided ready access to implement a redundant server infrastructure to allow for seamless failover. Previously, with on-premises installation at the State Data Center (SDC), FWC had limited access to our data and infrastructure; through Azure, we can access these servers through the Azure portal at any time.

- Security—Migration to Microsoft Azure provides greater control over security. We can restrict traffic on the network and application layers for private and public access, segregating portions of infrastructure and data.

- Scalability—Migration to the cloud provides FWC with robust scalability. FWC can increase computer storage, bandwidth, and security measures at a moment's notice.

- Monitoring—Migration to the cloud provides FWC with direct visibility into the server infrastructure for real-time data analytics and logging.

Scope/Business Objectives and Requirements

Historical Overview

FWC completed documenting the readiness, appropriate strategy, and high-level timeline for transitioning to a cloud-computing service.

The strategic plan requirements were identified by application; specifically, the plan identified and documented the readiness, appropriate strategy, and high-level timeline for transition to a cloud-computing service based on the application's quality, cost, and resource requirements.

FWC's plan for year one was to transition primarily to single system or application servers. This strategy proved successful and was expanded to include other items, including migrating the entire development environment to the Cloud.

During year two, FWC submitted a Legislative Budget Request for the 2021 session to transfer $483,790.68 in annual recurring funding from the Data Processing Assessment category to the Expenses category to fund the move from the State Data Center to the Cloud. This issue was funded and resulted in a net zero infrastructure cost change.

FWC migrated all user share data, comprising 18TB of data, to Microsoft OneDrive, which is included with our O365 subscription. FWC also migrated SharePoint 2010 to Microsoft Azure. These migrations resulted in six decommissioned servers at the State Data Center. Additionally, FWC continued its efforts to migrate its test and production application environments to Microsoft Azure and completed the migration in December 2021.

During year three, FWC submitted a Legislative Budget Request for the 2022 session to transfer $219,455.00 in annual recurring funding from the Data Processing Assessment category to the Expenses category to fund the move of Law Enforcement servers from the State Data Center to the Cloud. This issue was funded and resulted in a net zero infrastructure cost change. These were the last applications housed in the State Data Center, and they were successfully migrated. This completed our efforts to move from the State Data Center to the cloud successfully.

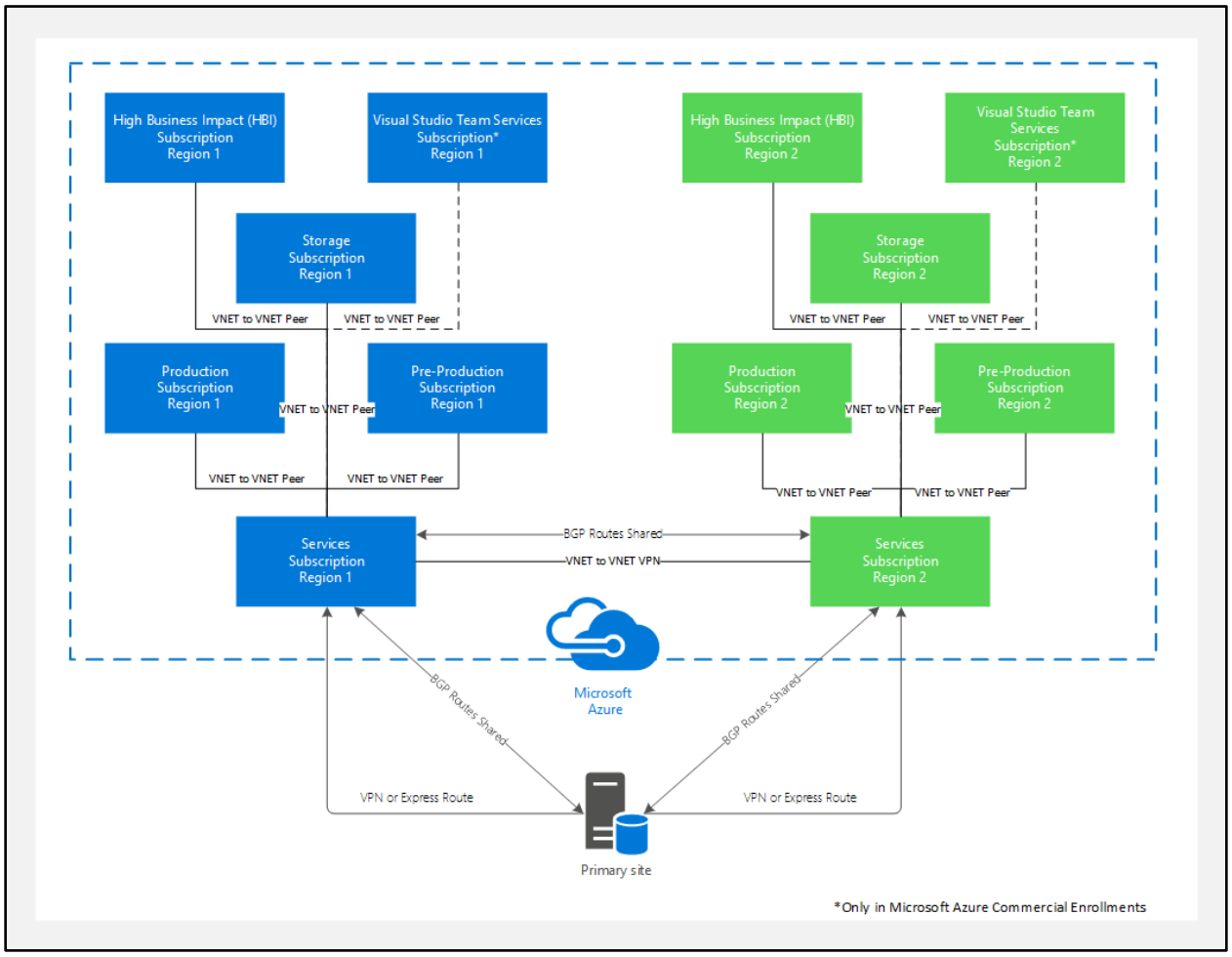
FWC did not submit a legislative budget request for FY23/24 for application modernization as we gathered, analyzed, and defined functional requirements. FWC made significant progress in evaluating low-code/no-code solutions, including completing a proof-of-concept application. We completed migrating to Azure SQL Managed Instance Database. We have updated and created new application applications using modern technologies [Permit Application, Red Snapper, etc.].

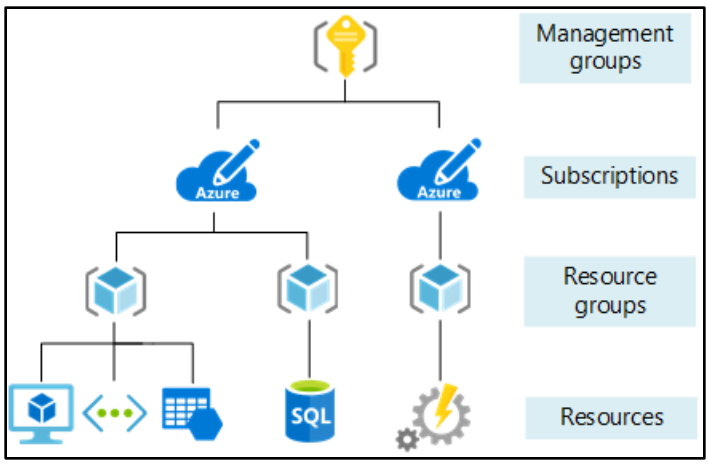
Current Year Strategy

FWC is targeting completing the migration of six existing applications from older technologies to modern technologies. Additionally, FWC will continue our efforts to move from multiple different applications/platforms to one unified platform, including expanding the FWC CRM to provide licensing that allows the public to access the information in the FWC CRM.

Architectural Overview

FWC's infrastructure is separated into 5 Azure virtual networks (Vnet.) These Vnets are divided into PreProd(Test), Development, Services, Production, and Storage. Each Vnet is logically segregated from the other. This allows for secure communications from the State of Florida's high-speed ExpressRoute for FWC traffic. This excludes traffic that FWC does not explicitly permit. FWC uses a subscription-based policy to provide role access security permissions for management access. The subscription services, network security groups, and firewall permissions have provided granular security and monitoring for access to the FWC virtual environment.





PEERS

Services – Primary hub and where the FWC VPN/ExpressRoute is terminated.
Production
Pre-Prod
Storage
HBI

SERVICES

The Services subscription is the only subscription that has connection endpoints for VPNs. All direct network connectivity to your Azure environment will be funneled through the Services subscription. The subscription methodology is laid out in a “hub and spoke” manner, Services is the hub of the hub and spoke model.

This subscription houses servers and services to be used by workloads spanning other Azure subscriptions. Examples include:

- Active Directory Controllers
- Domain Name Service (DNS)
- De-Militarized Zone (DMZ) type resources

Platform as a Service (PaaS) services monitor the Azure environment. Examples include:

- Log Analytics
- Azure Automation

PROD (PRODUCTION)

The Prod subscription is for production servers that would not qualify as HBI, Virtual Desktop Infrastructure (VDI), or Services resources.

PaaS services like Azure App Services will house Test, Development, and Production due to the nature of Deployment Slots.

PREPROD (PRE-PRODUCTION)

The PreProd subscription houses non-production workloads that need access to an on-prem network. PreProd is separated into Test and Development.

HBI

The HBI subscription is for production workloads with stricter network security and management access requirements. This data access should be limited to those with a direct business need to know. Examples include:

- Health Insurance Portability and Accountability Act (HIPAA)
- PCI – Payment Card Information
- PII – Personally Identifiable Information
- Authentication/Authorization Credentials

STORAGE

The Storage subscription is utilized for archival or tiered storage.

- Azure backup server for on-prem backups
- Azure Store Simple
- Marketplace appliances for Azure tiering volumes or archive storage.

FWC's cloud infrastructure and configuration follow Microsoft's best practices and those of other reputable third-party entities, such as Gartner and Airnet.

Backup Methodology

FWC implemented a robust backup policy for data that resides in Azure.

BACKUP FREQUENCY

Daily at 2:00 AM Eastern Time

Instant Restore

Retain instant recovery snapshot(s) for 2 days

RETENTION RANGE

Retention of daily backup point

Retain backup taken every day at 2:00 AM for 150 Days

Retention of weekly backup point

Retain backup taken every week on Saturday at 2:00 AM for 5 Weeks

Retention of monthly backup point

Retain backup taken every month on the First Sunday at 2:00 AM for 13 Months.

Retention of yearly backup point

Retain backup taken every year in January on the First Sunday at 2:00 AM for 7 Years.

Disaster Recovery

Migrating to Microsoft Azure has provided a secure and reliable way to perform Disaster Recovery utilizing replication to designated geo-located data centers across the Microsoft Azure United States data center footprint. This allows for backup jobs, servers, services, and access to be replicated in a one-to-one method while allowing for seamless failover.

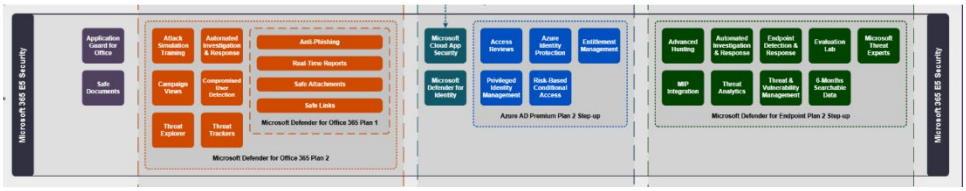
Data Security

Data Security—The Microsoft Cyber Defense Operations Center (CDOC) brings together security response experts from across the company to help protect, detect, and respond 24x7 to security threats against infrastructure and services in real-time. Specific to Florida, Microsoft is currently the only hyper-cloud service provider approved by the Florida Department of Law Enforcement (FDLE) for Criminal Justice Information Services (CJIS) compliance. This is a requirement for FWC.

FWC utilizes Microsoft's robust data security features to provide the following:

- **Identify-based access controls**—Features such as single sign-on and multi-factor authentication are built into Microsoft business products and services to protect information from unauthorized access while making it available to legitimate users whenever and wherever they need it.
- **Multi-tenant cloud environment**—Logical isolation with Azure Active Directory authorization and role-based control, data isolation mechanisms at the storage level, and rigorous physical security. Encryption serves as the last and most vital line of defense. Microsoft utilizes strong, secure encryption protocols to safeguard customer data and help maintain control.
- **Threat Protection**—Exchange Online Protection's deployment across a global network of data centers enables email protection from multi-layered, real-time anti-spam to multi-engine antimalware protection. Microsoft antimalware for Azure cloud services and virtual machines provides real-time protection capability to identify and remove viruses, spyware, and other malicious software.
- **Auditing and logging of security-related events**—Microsoft business services and products provide configurable security auditing and logging options to help identify gaps in security policies and mechanisms and address those gaps to help prevent breaches. FWC is utilizing Microsoft services as follows:
    - centralized monitoring
    - logging
    - analysis systems to provide continuous visibility, timely alerts, and reports to help manage the large volume of information generated by devices and services

- **Microsoft 365 E5 security**



- **Identity**
  - Privilege Identity protection
  - Azure Identity Protection
  - Entitlement Management
  - Risk-based conditional access
  - Risky user reporting
- **Microsoft Defender for cloud/endpoint**
  - Automated investigation and response
  - Endpoint Detection and Response (EDR)
  - Advanced threat analysis and threat hunting
  - Threat and vulnerability management
- **Defender for Office 365**
  - Anti-phishing
  - Safe attachments
  - Safe links
  - Compromised user detection
  - Attack simulation training
- **Microsoft Defender for Cloud**
  - Manage compliance against critical industry standards
  - Regulatory compliance
  - Threat protection workbooks.
  - Vulnerability detection
  - Security posture and alerts
  - Workload protections and recommendations
  - Vulnerability assessments
  - Adaptive Application control
  - SQL vulnerability assessments
  - Azure inventory management
- **Azure Firewall**
  - TLS inspections
  - Intrusion detection and prevention system
  - URL filtering

Training

FWC's training program for this reporting period was structured around Microsoft's Enterprise Skills Initiative. This program was tailored to provide skills training specific to each staff member to support cloud environments and application modernization. To increase the upskilling initiative, FWC will leverage proactive credits in the Microsoft Unified Support contract for application modernization/cloud application workshops. See the example slides below that represent a training plan for an FWC Data Automation Specialist and an FWC Application Developer:

Upskilling Data automation employees at FWC

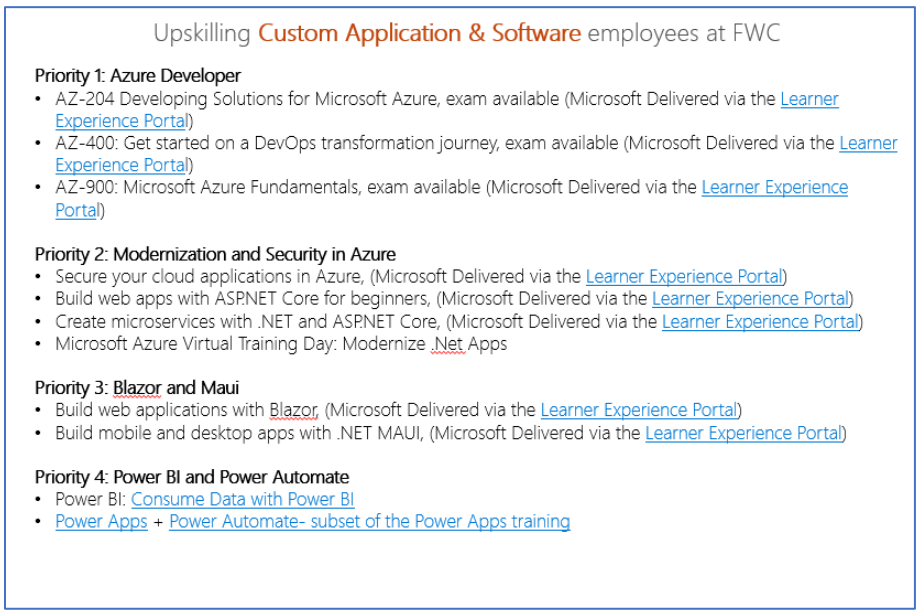
Priority 1: Laserfiche Gold certification
- Getting started with Laserfiche and document capture
- Using and designing Laserfiche forms
- Using quick fields sessions and workflows
- System administration 1 &2

Priority 2: PPL
- Power Platform Fundamentals via Training Days in Learner Experience Portal or MS Learn, exam available
- Power Apps + Power Automate- subset of the Power Apps training
- Integrate SharePoint and Power Automate

Priority 3: Dax and Advanced Data Analysis
- Use Dax in Power BI Desktop available in MS Learn, 2.5 hours
- DA-100 Analyzing Data with Microsoft Power BI, Microsoft Delivered through Learner Experience Portal, exam available
  - Prereq: MS Azure Data Fundamentals via Training Days in Learner Experience Portal or MS Learn

Priority 4: Teams – Explore content for relevant competency areas:
- Training Days in Learner Experience Portal available now:
  - Enable Remote/Hybrid work with MS Teams
  - Building MS Teams Integrations and Workflows

Priority 5: Security
SC-400 Information Protection Administrator, instructor led via the Learner Experience Portal
  - Prereq: SCI Basics, Azure Basics, M365 Basics



Upskilling Custom Application & Software employees at FWC

Priority 1: Azure Developer
- AZ-204 Developing Solutions for Microsoft Azure, exam available (Microsoft Delivered via the Learner Experience Portal)
- AZ-400: Get started on a DevOps transformation journey, exam available (Microsoft Delivered via the Learner Experience Portal)
- AZ-900: Microsoft Azure Fundamentals, exam available (Microsoft Delivered via the Learner Experience Portal)

Priority 2: Modernization and Security in Azure
- Secure your cloud applications in Azure, (Microsoft Delivered via the Learner Experience Portal)
- Build web apps with ASP.NET Core for beginners, (Microsoft Delivered via the Learner Experience Portal)
- Create microservices with .NET and ASP.NET Core, (Microsoft Delivered via the Learner Experience Portal)
- Microsoft Azure Virtual Training Day: Modernize .Net Apps

Priority 3: Blazor and Maui
- Build web applications with Blazor, (Microsoft Delivered via the Learner Experience Portal)
- Build mobile and desktop apps with .NET MAUI, (Microsoft Delivered via the Learner Experience Portal)

Priority 4: Power BI and Power Automate
- Power BI: Consume Data with Power BI
- Power Apps + Power Automate- subset of the Power Apps training

Contractual Considerations

Performance Monitoring

FWC leverages the Azure Monitor services with all services/applications migrated and deployed to the Microsoft Cloud. Services include:

- Detect and diagnose issues across applications and dependencies with Application Insights.
- Correlate infrastructure issues with Azure Monitor for VMs and Azure Monitor for Containers.
- Drill into your monitoring data with Log Analytics for troubleshooting and deep diagnostics.
- Support operations at scale with smart alerts and automated actions.
- Create visualizations with Azure dashboards and workbooks.

Exit Strategy

FWC has full rights to migrate to and from the Microsoft Cloud as needed without penalties. If/when required, FWC will ensure proper planning to execute such a strategy.

Service Level Agreements

All service level agreements are provided by Microsoft per service as described here:

- at least 99.9% availability of the Azure Active Directory Basic and Premium services
- at least 99.9% of Azure Active Directory Domain Services
- Applications running in a customer subscription will be available 99.95% of the time

Legislative Budget Request

FWC did not submit a legislative budget request for cloud migrations for FY24/25, as that work has been completed.

FWC submitted a legislative budget request (LBR) for application modernization for FY24/25. This issue requested budget authority in the Contracted Services appropriation category for $375,000 in the Administrative Trust Fund (ATF).

The requested funds will supplement our current staff in modernizing and maintaining FWC's 124 applications to support better application security, performance, and functionality.

FWC also submitted an LBR for $400,00 in the Administrative Trust Fund (ATF) and budget authority in the Expense appropriation category for $254,00 in the Administrative Trust Fund (ATF) to continue implementing and supporting the FWC enterprise CRM platform.

FWC's continued successful modernization efforts depend upon the approved funding of these Legislative Budget Requests.

Application Modernization Plan

When FWC formalized our plan to move to the cloud, we faced a decision point on modernizing our applications pre-migration or post-migration. We modernized our post-migration applications to expedite migration from the state data center. After migrating all servers and systems to the cloud, we have moved on to upgrading our applications. Phase One (Defining, Evaluating, and Planning) will take two years to complete.

As we started the first phase of our modernization process, FWC analyzed our applications and determined that 72 FWC-maintained applications would require modernization. During the first year of Phase One, we targeted moving 29 applications to DevOps. We have completed that effort.

During the second year of Phase One, we completed evaluating low-code/no-code solutions and have identified the first six applications to migrate from our older technologies to a modern low-code/no-code solution.

This will move FWC into Phase Two (Execution). During the upcoming year, FWC targets completing the migration of six existing applications from older to modern technologies.

Completed Items

The following pages reflect the current Application Modernization Plan.

App	Deploy to DevOps
Bear sightings	Complete
Bobwhite Quail Sightings	Complete
CatchaFloridaMemory.com	Complete
Chipmunk Sightings	Complete
Commercial Fresh/Salt License Public Record Export Process	Complete
Commission Meeting Registration	Complete
Departed Users Automated Access Deactivation	Complete
FishKillReport	Complete
FishKillSearch	Complete
FishKillUpload	Complete
FWC Employee Validator	Complete
FWC Master Theme	Complete
FWC Web Site (MyFWC)	Complete
Google Maps for Enterprise	Complete
Gopher Tortoise Permit Map	Complete
Gopher Tortoise Sightings	Complete
Grass Carp Permitting System	Complete
Great Florida Birding & Wildlife Trail - Mapping	Complete
Hunter Safety > GOF Daily Export	Complete
Invasive Plant Management IPM (Sync Service / Toolbar)	Complete
LMIS Area Managers Tools AMT (Sync Service / Toolbar)	Complete
NOAA Recreational License Export-Transfer Process	Complete

App	Deploy to DevOps
Object-Based Vegetation Management (OBVM) - Land Management Information System	Complete
Panther Sightings	Complete
Public Records Exemption Information System	Complete
Rare Snake Sightings	Complete
Rare Upland Birds	Complete
Weasel Sightings	Complete
Wildlife Alert Application	Complete

To Complete Items

App	Migrate to Modern Technology
Bobcat Mortality	In Process
Exotic Pet Amnesty	In Process
FWC Permit System	In Process
FYCCN Summer Camp Registration	In Process
Panther Incidents	In Process
VEMS	In Process
Angler Recapture	Not Started
ArrestNet Boating Accidents	Not Started
ArrestNet Security - Menu of LE Applications	Not Started
ArrestNet Ticket Tracking	Not Started
Avian Mortality	Not Started
BARD Web Service	Not Started
Bear sightings	Not Started
Bobwhite Quail Sightings	Not Started
Buck Registry	Not Started
CatchaFloridaMemory.com	Not Started
Chipmunk Sightings	Not Started
Commercial Fresh/Salt License Public Record Export Process	Not Started
Commission Meeting Registration	Not Started
Departed Users Automated Access Deactivation	Not Started
Fish Health Reporting (incorporated into FWC Reporter app)	Not Started
Fisheries Dependent Monitoring (FDM/MRIS)	Not Started
FishKillReport	Not Started
FishKillSearch	Not Started
FishKillUpload	Not Started
Florida Reef Resiliency Program (FRRP)	Not Started
Florida Shorebird Database/Beach-nesting birds (Internet)	Not Started
FWC Employee Validator	Not Started

App	Migrate to Modern Technology
FWC Master Theme	Not Started
FWC Reporter App	Not Started
FWC Web Site (MyFWC)	Not Started
Google Maps for Enterprise	Not Started
Gopher Tortoise Permit Map	Not Started
Gopher Tortoise Sightings	Not Started
Grass Carp Permitting System	Not Started
Great Florida Birding & Wildlife Trail - Mapping	Not Started
Harmful Algal Bloom Database (HAB)	Not Started
Horseshoe Crab	Not Started
Hunter Safety > GOF Daily Export	Not Started
Hunting WMA Brochures DB	Not Started
Integrated Tracking of Aquatic Animals in the Gulf of Mexico (ITAG)	Not Started
Invasive Plant Management IPM (Sync Service / Toolbar)	Not Started
JEA (Joint Enforcement Agreement)	Not Started
LEX	Not Started
LMIS Area Managers Tools AMT (Sync Service / Toolbar)	Not Started
Long-Term Monitoring	Not Started
Manatee Mortality Data Upload (ManateeUpload)	Not Started
Manatee Mortality Report (ManateeReport)	Not Started
MetaRep	Not Started
NOAA Recreational License Export-Transfer Process	Not Started
Object-Based Vegetation Management (OBVM) - Land Management Information System	Not Started
OIT Task Tracker-Work Log	Not Started
Panther Sightings	Not Started
PersonnelNet	Not Started
Plant Management Aquatic Reporting System (PMARS 2)	Not Started
Plant Management Research, Outreach Online Tracking (R & O) System	Not Started
Plant Management Upland Reporting System (TIERS)	Not Started
Property Master Daily Import Job	Not Started
Public Fisheries Dependent Monitoring (PFDM)	Not Started
Public Records Exemption Information System	Not Started
Publications Management System	Not Started
Rare Snake Sightings	Not Started
Rare Upland Birds	Not Started
Research Approval Form	Not Started
RFI (Request for Information)	Not Started
SEAMAP	Not Started
Species Ranking	Not Started

App	Migrate to Modern Technology
State Wildlife Grants Funded Projects (Internet)	Not Started
Stolen Vessel-FCIC/HSMV Data - LE	Not Started
Stone Crab	Not Started
Survey and Monitoring Protocol	Not Started
Tech Staff Module (Desktop)	Not Started
Watercraft Safety	Not Started
Weasel Sightings	Not Started
Wildlife Alert Application	Not Started
WMA Activity Planning and Reporting Databases (Intranet)	Not Started
WMA Harvest Database	Not Started
WMA Hunting	Not Started