# CJIS Cloud Migration

Brian Griffith

IT Management Section Chief

CJIS Division

# Why Cloud?

### *INNOVATION*

- Innovate more quickly and with more relevance than three-to-five-year technology refresh cycles

### *RESOURCE ALLOCATION*

- Quickly allocate new resources, avoiding long hardware procurement lead times

### *BUSINESS SOLUTIONS*

- Focus resources on solving business problems rather than procuring and configuring physical infrastructure

### *WASTE REDUCTION*

- Avoid wasted resources for off hours when designing for peak loads by automatically scaling resources up and down as needed

### *FEDERAL/AGENCY MANDATES*

- *OMB, DOJ, & FBI "Cloud First" directives*

### *ACCESS TO NEW TECHNOLOGIES*

- Access upgraded hardware as it becomes available from cloud providers
- *ACCESS TO NEW TECHNOLOGIES*
  - Access upgraded hardware as it becomes available from cloud providers

### *CULTURE CHANGE*

- Adapt legacy mindset to application development and maintenance with modern techniques (Infrastructure as Code, DevOps, etc.)

### *STANDARDIZATION*

- Help standardize technology footprints using a more consistent set of tools

### *TECHNICAL DEBT ELIMINATION*

- Succeed in meeting mission and business goals by reducing technical debt

# CJIS systems began cloud migrations in 2017 and are migrating in a variety of ways:

## Hybrid Operations

- Migrate pieces of functionality to cloud, with remaining pieces on existing on-premise hardware
  - NGI – Latent fingerprint matching
  - N-DEx – Document search engine

## Continuity of Operations

- Move backups/offsite storage to the cloud
  - CJIS Object Store – Replication site in Cloud
  - CJIS Enterprise Backup Services (EBS) – Moving offsite backups to Cloud

## Full Deployment

- Operate fully in the cloud
  - XML Conformance Testing Assistant (XCOTA) – full system in Cloud

# Major Migration Successes


***What We Migrated:***

- COTS fingerprint matching solution for latent fingerprints
- On-demand "push button" development environments (build & destroy)
  - Deployed as Kubernetes PaaS with SNS and ElastiCache

***Size:***

- Represents 50% of NGI's on-premise compute footprint
- Each matching unit (four total – three as reserved instances and one on-demand) includes 30 compute/memory-intensive EC2 instances

***Obstacles Overcome:***

- The number of large instances required for each matching unit exhausted GovCloud West on-demand EC2 availability. Reserved Instances solved this problem.

***Benefits Realized:***

- Removed ~1,000 on-premise servers, simplifying O&M workload
- Cost benefit realized by reducing overall size of NGI latent deployment because of the ability to scale as needed


***What We Migrated:***

- COTS document search engine solution (MicroFocus IDOL)
- ElasticStack (ELK) application monitoring infrastructure

***Size:***

- Represents 68% of N-DEx's on-premise compute footprint
- ~300 EC2 instances procured via Reserved Instances

***Obstacles Overcome:***

- Proper sizing estimate required several rounds of performance testing

***Benefits Realized:***

- Ability to rapidly reconfigure/redeploy instance types accelerated instance evaluation
- Increased performance relative to resources used
- Production resiliency
- Scalability & responsiveness

# Major Migration Successes

CJIS Object Store

| What We Migrated: | Obstacles Overcome: |
|---|---|
| ▪ Replaced Disaster Recovery site for CJIS Object Store<br>▪ Stores fingerprints, mugshots, police reports, etc.<br>***Size:***<br>▪ 18 Billion objects<br>▪ 2.5 PB storage<br>▪ 300 new/updates per second | ▪ Hot migration of live system (servicing NGI and N-DEx)<br>▪ Replicated onsite objects over the wire while maintaining consistency of creates/updates/deletes<br>***Benefits Realized:***<br>▪ Refactored to leverage cloud-managed services (Oracle RDBMS replaced with DynamoDB and RDS)<br>▪ Dynamically scaled compute, storage, and database capacity<br>▪ Cloud services provided access to features not available on-premise |

Xcota

| What We Migrated: | Obstacles Overcome: |
|---|---|
| ▪ Online Data Standards Website<br>▪ https://datastandards.cjis.gov<br>***Size:***<br>▪ ~10 servers | ▪ Engineering security stack (DMZ/AWS DirectConnect/VPC configuration/etc.) for a public website through the TIC<br>***Benefits Realized:***<br>▪ Less time and labor spent on capacity planning<br>▪ Less time and labor spent on logistics (hardware install/ configuration)<br>▪ Increased efficiency in security assessments<br>▪ Built-in tech refresh |

# Future Migrations

Ten-print matching subsystem to Cloud later this year

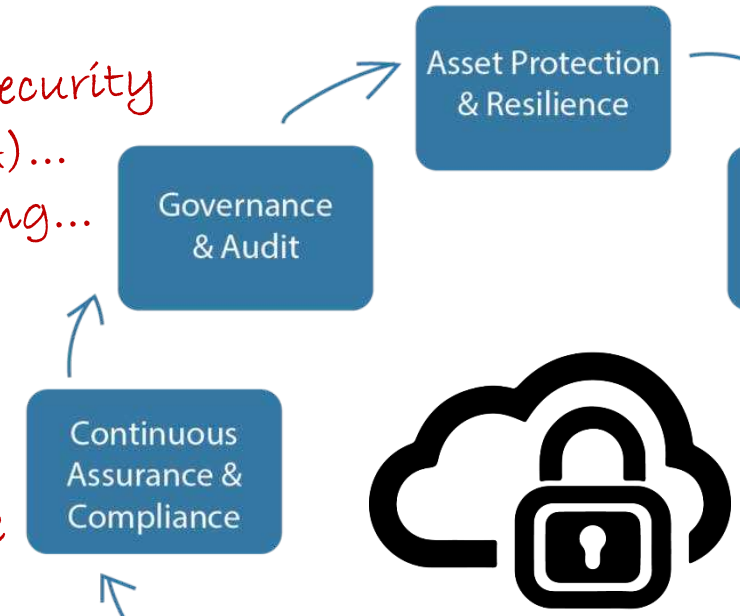
First phase of functionality in Cloud early next year

Entity resolution/ correlation engine to Cloud later this year

Migration planning after successful proof of concept for tactical and offline searches

First phase of functionality in Cloud early next year

Design for resilience
FedRAMP Moderate/High only




ATO compliance &
Automated Cloud Security
Assessment (ACSA)…
Inventory monitoring…

Encryption w/
key management

Planned for…
Least privileged user…
Automation…

Type-accredited
VPC framework &
Transit VPC…
TIC enforcement…

Federated, role-based IAM w/
two-factor authentication

Restricted

Standard security
scanning tools
& code review…
Configuration change
notification…

# Cloud Security Best Practices

- ❑ Must only use FedRAMP High Government Community Cloud
  - ❑ JAB accredited; 3PAO audited; continuous monitoring controls
  - ❑ Facility, Personnel and Infrastructure control inheritance
- ❑ Services must also be approved at FedRAMP High
- ❑ Data must be encrypted at rest
- ❑ Data must be encrypted in transit
- ❑ Encryption keys must be managed by LEA
  - ❑ AWS Key Management Service and Azure Key Vault are FedRAMP High
- ❑ All authentication 2-Factor
- ❑ Processing within a secure Virtual Private Cloud (VPC)
- ❑ Internet access to/from VPC through secure transit gateway
- ❑ Least Privileged User approach to roles for account permissions
- ❑ …

***Note**: It is the responsibility of the client (agency) to ensure that appropriate controls surrounding VPC access, roles, identities, and privileges are designed and implemented properly. If any of these is poorly implemented, physical and logical controls to prevent access to CJI by the Cloud Service Provider, or anyone, are meaningless.*
***It is not the Cloud Service Provider's job to secure client data.***