



Federal Bureau of Investigation

Criminal Justice Information Services (CJIS) Division



Advisory Process



Shared Management Concept

- Federal, state, local, and tribal users and providers share the responsibility for the operation and management of systems administered by the CJIS Division for the benefit of the criminal justice community.

CJIS Advisory Process

- Process to obtain the user community's guidance on the operation of CJIS programs.

CRIMINAL JUSTICE INFORMATION SERVICES (CJIS) SYSTEMS USER AGREEMENT

The FBI CJIS Division provides state-of-the-art identification and information services to the local, state, tribal, federal, and international criminal justice communities, as well as the noncriminal justice community, for licensing and employment purposes. These services are administered and maintained by the FBI CJIS Division and managed in cooperation with the CJIS Systems Agency (CSA) and its administrator for CJIS data, the CJIS Systems Officer (CSO). The CJIS Systems include, but are not limited to: the Interstate Identification Index (III); National Crime Information Center (NCIC); Uniform Crime Reporting (UCR), whether summary or incident-based reporting to the National Incident-Based Reporting System; Fingerprint Identification Record System; Law Enforcement National Data Exchange (N-DEX); Law Enforcement Online; and the National Instant Criminal Background Check System (NICS). The FBI CJIS Division provides the following services to its users, as applicable:

1. Operational, technical, and investigative assistance.
2. Telecommunication lines to state, federal, and regulatory interfaces.
3. Legal and legislative review of matters pertaining to all CJIS Systems.
4. Timely information on all aspects of all CJIS Systems and other related programs by means of operating manuals, code manuals, technical and operational updates, various newsletters, information letters, frequently asked questions, and other relevant documents.
5. Training assistance and up-to-date materials provided to each CSO, NICS Point of Contact (POC), state Compact Officer, State Administrator, Information Security Officer (ISO), and other appropriate personnel.
6. Ongoing assistance to Systems' users through meetings and briefings with the CSOs, State Administrators, Compact Officers, ISOs, and NICS State POCs to discuss operational and policy issues.
7. Advisory Process through which authorized users have input as to the policies and procedures governing the operation of CJIS programs.
8. National Crime Prevention and Privacy Compact Administrative Office through which states and other authorized users may submit issues concerning the noncriminal justice use of the III System.
9. Annual NICS Users Conference.
10. Audit.
11. Staff research assistance

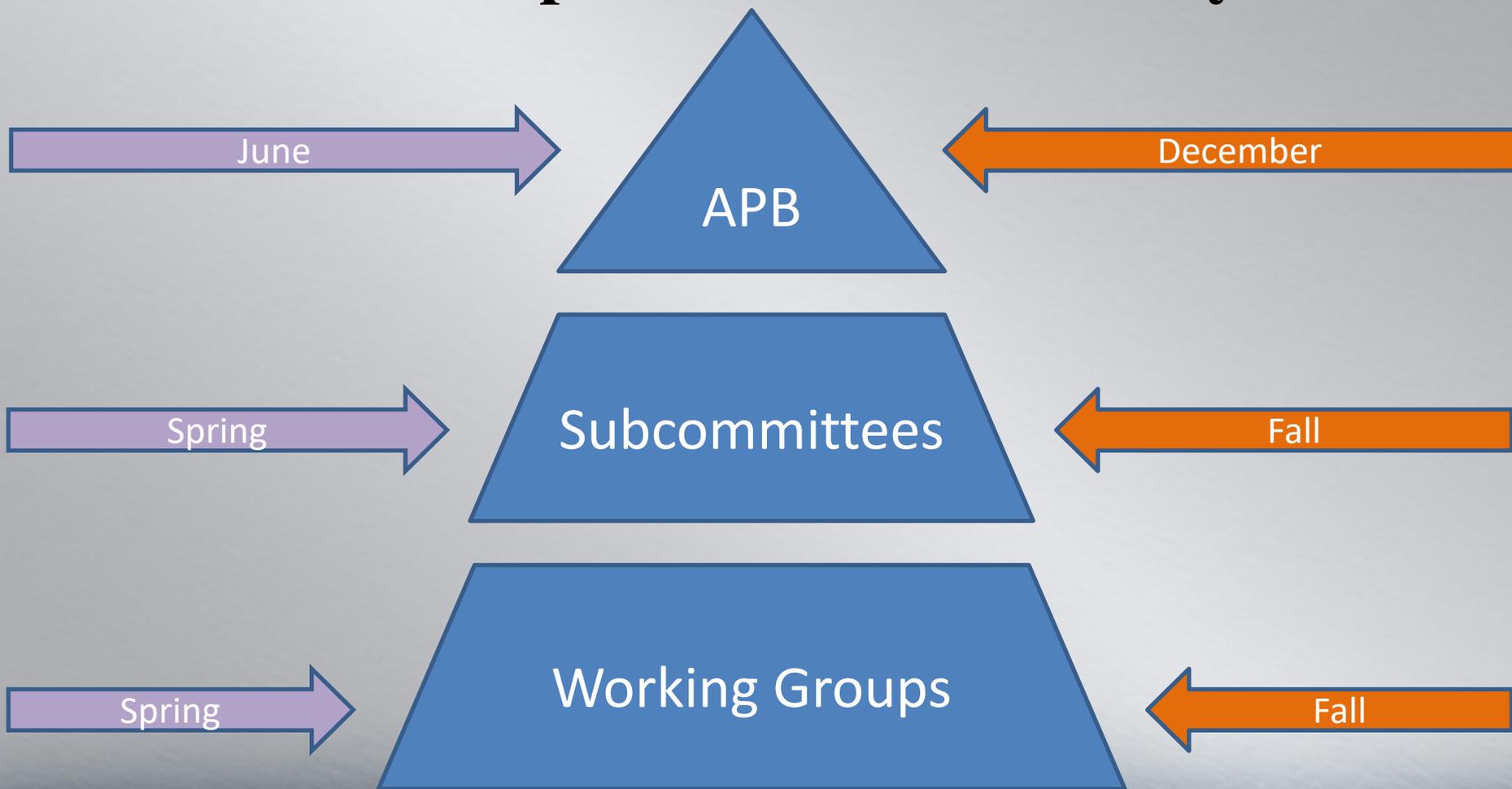


FBI CJIS Services

- National Crime Information Center (NCIC)
- Next Generation Identification (NGI)
- Uniform Crime Reporting (UCR)
- National Data Exchange (N-DEx)
- Law Enforcement Enterprise Portal (LEEP)
- National Instant Criminal Background Check System (NICS)



Three Main Components of the Advisory Process

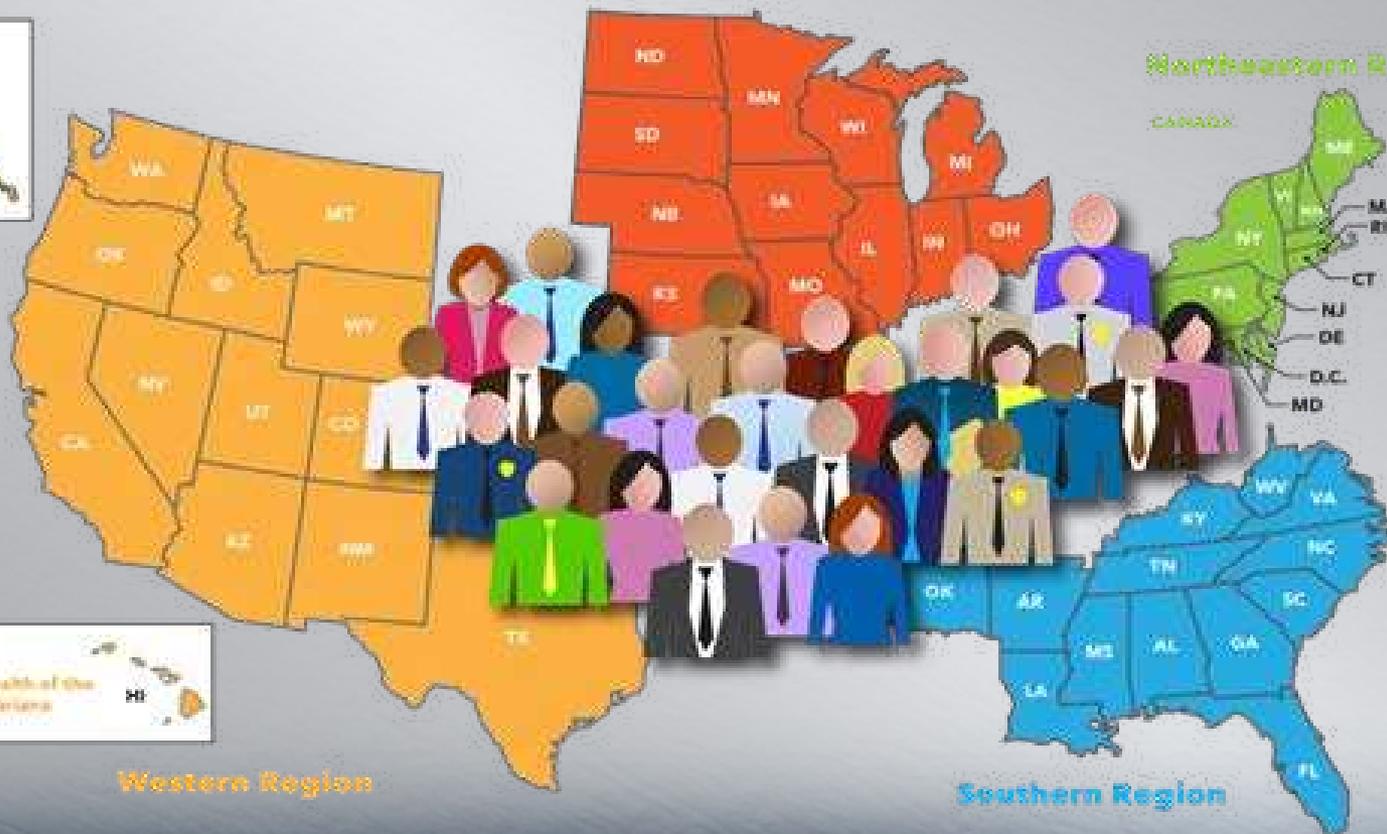




Advisory Policy Board Working Groups Regions Map

North Central Region

Northeastern Region



Western Region

Southern Region

UNCLASSIFIED

Source: FBI/DOJ
U.S. Virgin Islands



Working Group Roles and Responsibilities

Local Agency Representative Responsibilities:

- Represent the interests of the CJIS Advisory Process during meetings/conferences with criminal justice agency representatives in their state in order to solicit topics for discussion to improve the CJIS Division systems
- Represent the view of all local agencies in their states on issues being addressed during WG meetings
- Attend all WG meetings
 - If unable to attend, notify WG Chair of plans to send proxy.

State / Federal Agency Representative Responsibilities:

- Represent the views of the CSA concerning issues being addressed during WG meetings
- Represent the views of all agencies in the department/state on issues being addressed during WG meetings and keep agencies informed of current issues
- Attend all WG meetings
 - If unable to attend, notify WG Chair of plans to send proxy.



CJIS Subcommittees

- Subject matter experts assembled to thoroughly review policies, issues, program changes, and formulate alternatives for APB consideration
- January reconstitution



Subcommittees

- Bylaws
- Identification Services (IS)
- National Data Exchange (N-DEx)
- National Crime Information Center (NCIC)
- Compliance Evaluation
- Security and Access
- Uniform Crime Reporting (UCR)
- National Instant Criminal Background Check System (NICS)
- **Executive**



FBI CJIS APB

- The Advisory Process is the mechanism by which the FBI Director receives advice and guidance on the operation of the CJIS systems.
- The APB is chartered under the Federal Advisory Committee Act (FACA).
 - Every 2 years the Charter is renewed
- The APB (as it is shaped today) was first chartered in 1994
 - Combination of existing National Crime Information Center (NCIC) APB and Uniform Crime Report (UCR) APB.



The APB FACA

- Chartered by the Attorney General
 - Filed with Congress
- Meeting Requirements
 - Public attendance
 - Public participation
 - Access considerations
- Meeting Documentation
 - Certified minutes



The APB is made up of 35 members:

(20) Selected by the four Regional Working Groups

(1) Selected by the Federal Working Group

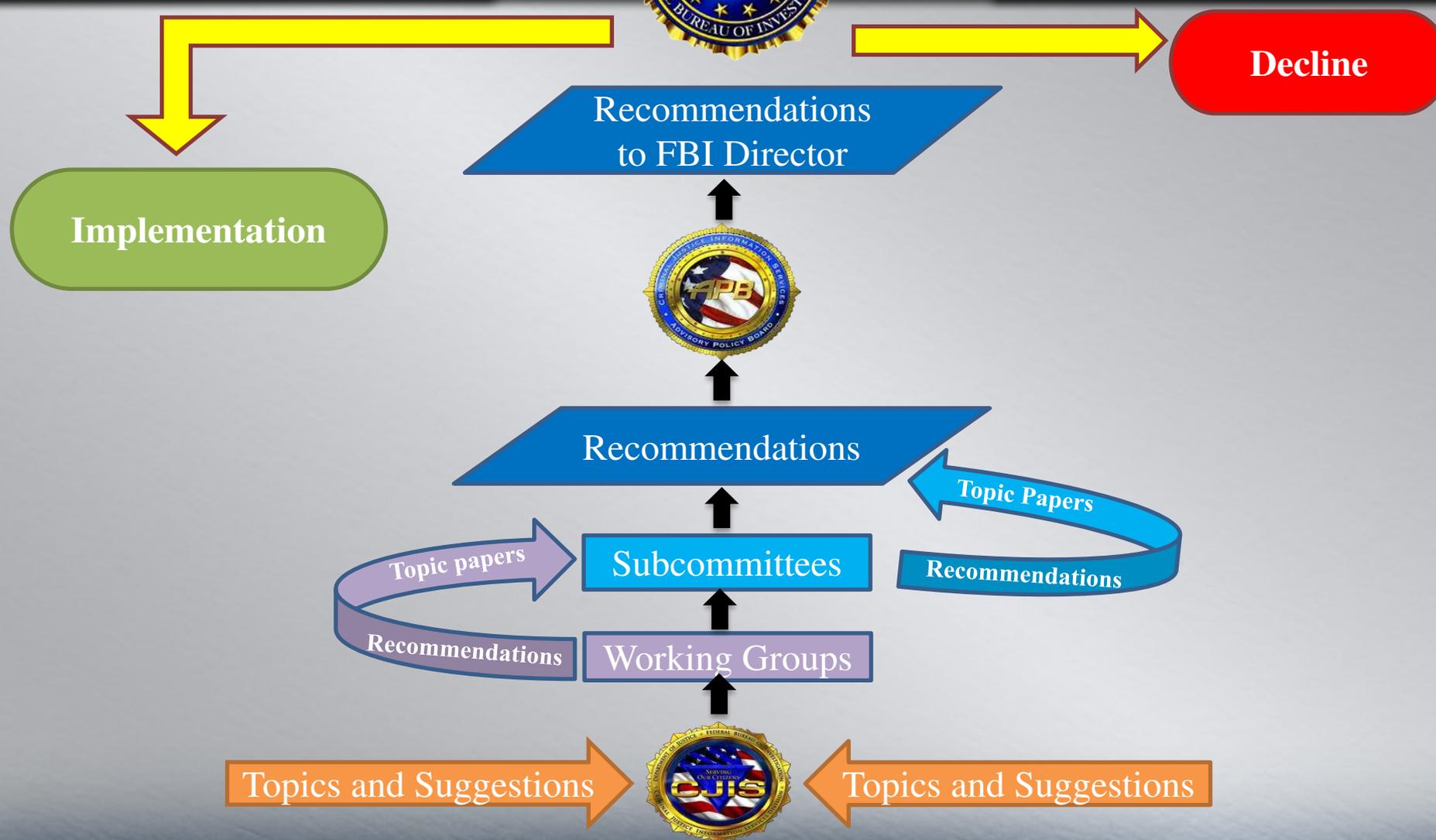
(5) FBI Director appointees

- 1 judiciary representative
- 1 prosecutorial representative
- 1 correctional representative
- 1 national security representative
- 1 tribal law enforcement representative

(8) Professional Criminal Justice Association representatives

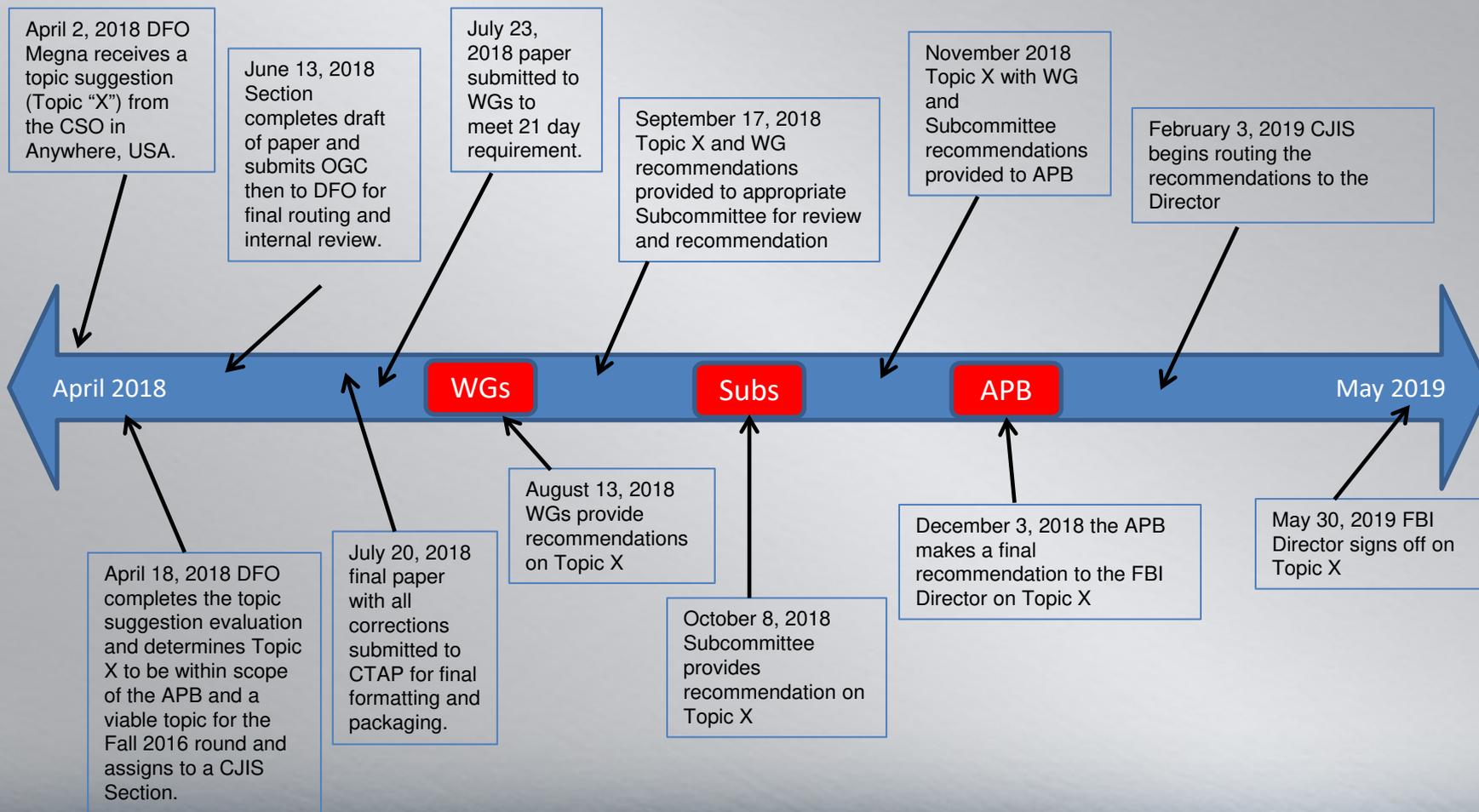
- International Association of Chiefs of Police (IACP)
- National Sheriffs' Association (NSA)
- National District Attorneys' Association
- American Probation and Parole Association
- Major Cities Chiefs' Association
- Major County Sheriffs' Association
- American Society of Crime Laboratory Directors
- Courts or Court Administrators chosen by the Conference of Chief Justices

(1) National Crime Prevention and Privacy Compact Council representative





APB Sample Topic Timeline





Questions?

Nicky J. Megna
Designated Federal Officer
FBI CJIS Division
Phone: 304-625-5263
E-mail: <njmegna@fbi.gov>



Information Technology Security (ITS) Audit

Audit Summary

Candice B. Preston / Ronnie L. George
CJIS Audit Unit
(304) 625 – 5557 / (304) 625 – 2632

CJISAUDIT@fbi.gov



Audit Findings

Criminal Justice Agency Findings Summary



Background

October 1, 2017 through September 30, 2018

– 252 Total Agencies

- 25 CJIS Systems Agencies (CSAs)
 - 18 States
 - 7 Federals
- 227 Local Agencies



Criminal Justice Agency

October 2017 – September 2018



Rank	Policy Area	Noncompliance Rate
1	Event Logging	42 %
2	Encryption	35 %
3	Advanced Authentication	33%
4	Identification/UserID	29 %
5	System Use Notification	29 %
6	Management Control Agreements	28 %
7	Security Addendums	27 %
8	Security Awareness Training	25 %
9	Personally Owned Information Systems	24 %
10	Media Disposal	22 %



Repeat Offenders



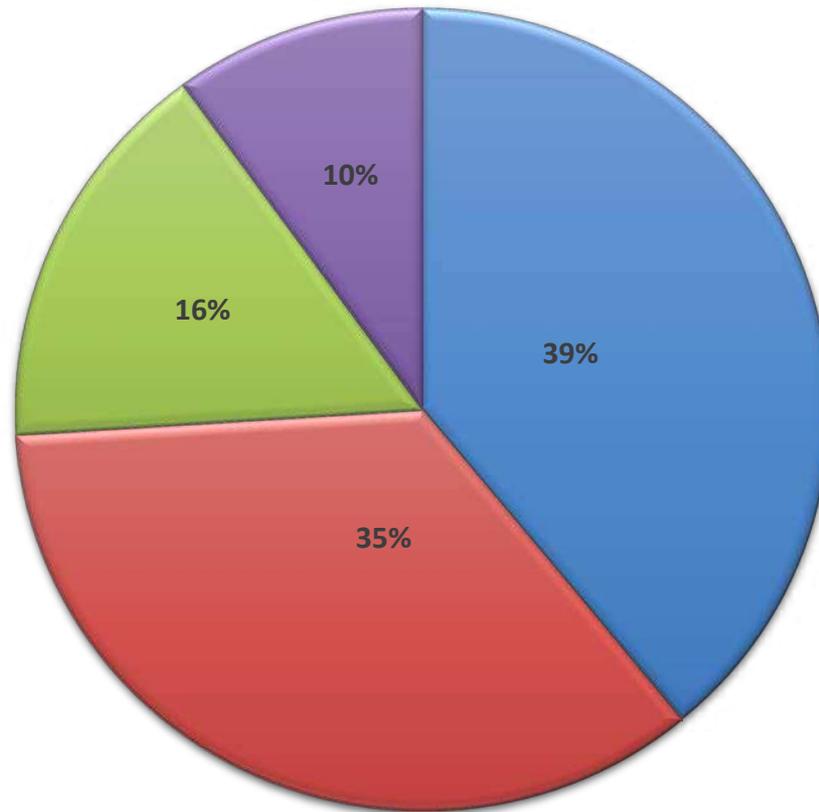
Top Findings
Event Logging
Encryption
Advanced Authentication
Identification/UserID
System Use Notification
Management Control Agreements
Security Addendums
Security Awareness Training



Breakdown Criminal Justice Agencies

Percentage of Event Logging OUTs

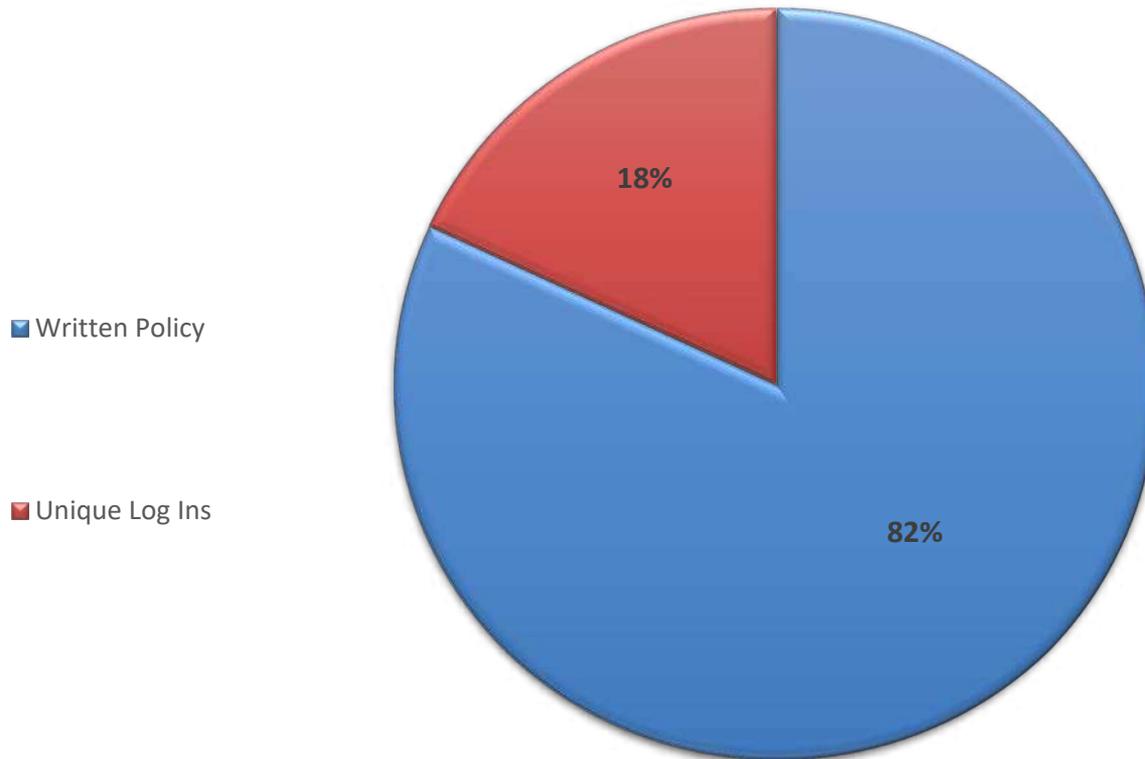
- No weekly review
- No logging/Not logging required events
- Logging failure does not provide alerts
- Log Retention





Breakdown Criminal Justice Agencies

Percentage of Identification/UserID OUTs

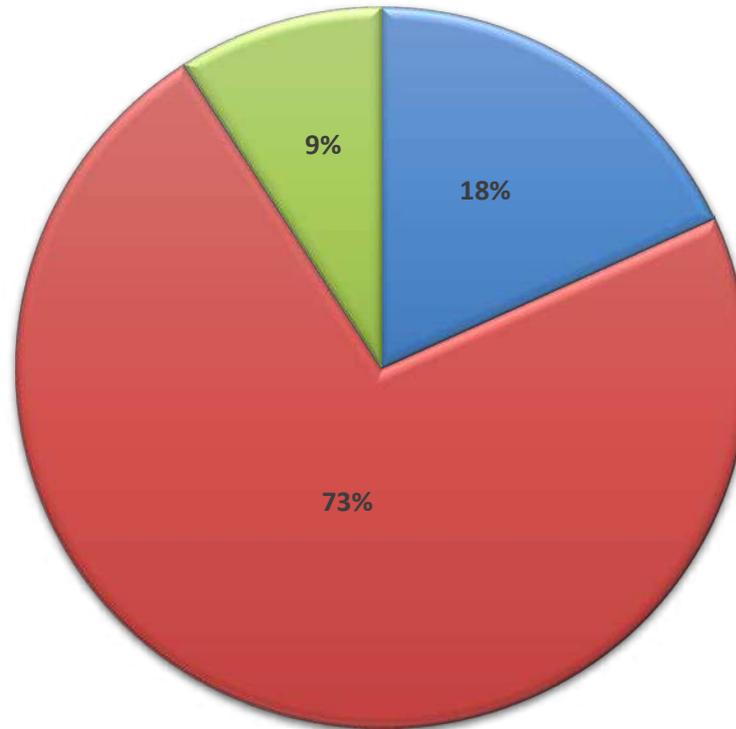




Breakdown Criminal Justice Agencies

Percentage of Media Disposal OUTs

- Release of Hard Drives without Wipe
(leased/rented copiers)
- Written Policy
- Physical Media Destruction not
witnessed by Authorized Personnel

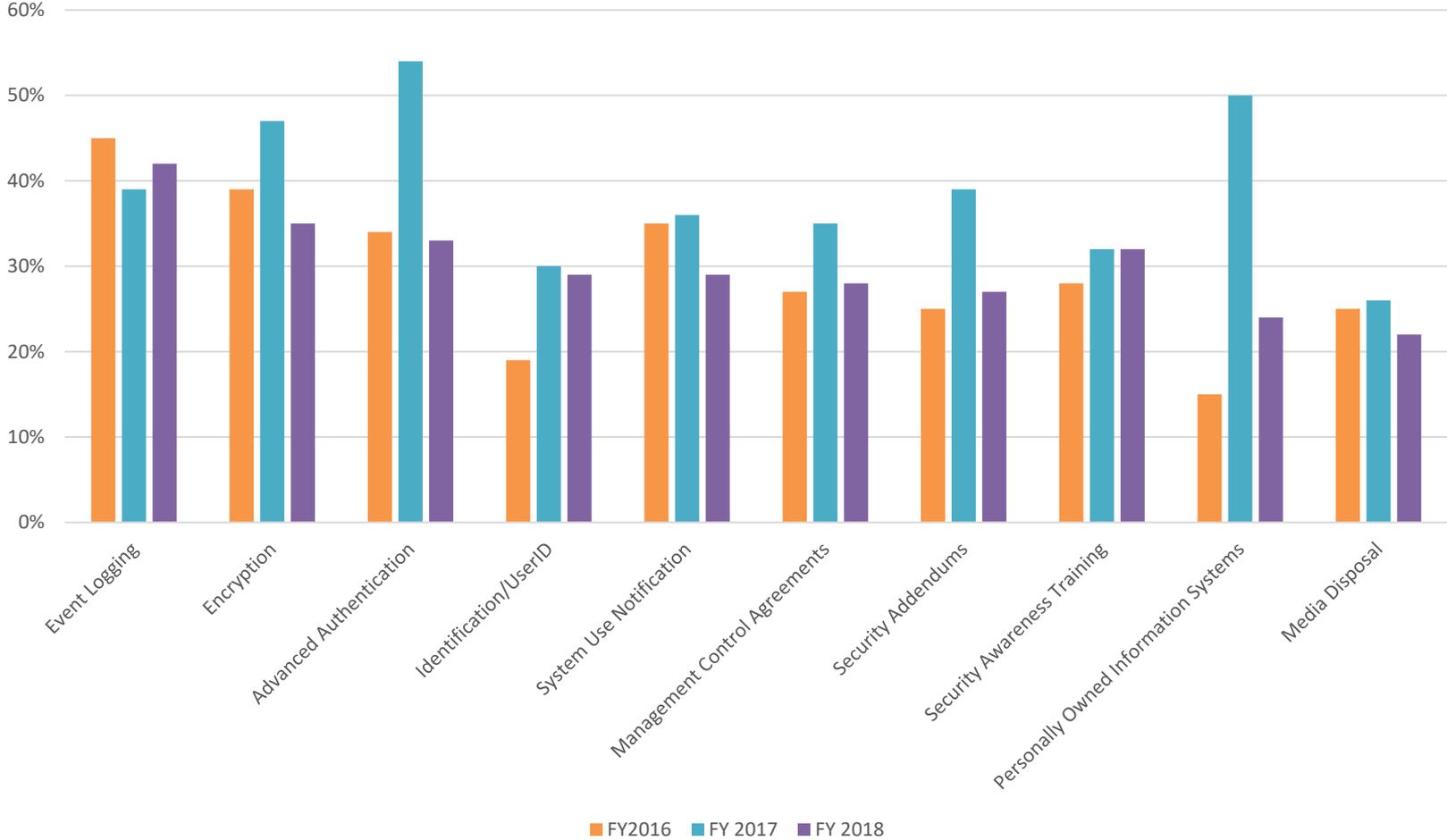




Criminal Justice Agency Trends



Criminal Justice Agency Trends





Audit Findings

Noncriminal Justice Agency Findings Summary



Background

October 1, 2017 through September 31, 2018

– 129 Total Agencies

- 17 CJIS Systems Agencies (CSAs)
- 112 Local Agencies



Noncriminal Justice Agency October 2017 – September 2018



Rank	Policy Area	Noncompliance Rate
1	Contracted Noncriminal Justice Functions	89 %
2	Event Logging	53 %
3	Encryption	45 %
4	Personally Owned Information Systems	39 %
5	Media Disposal	35 %
6	Security Awareness Training	31 %
7	Security Audits	30 %
8	Physical Security	29 %
9	Mobile Devices	26 %
10	Identification/UserID	24 %



Repeat Offenders



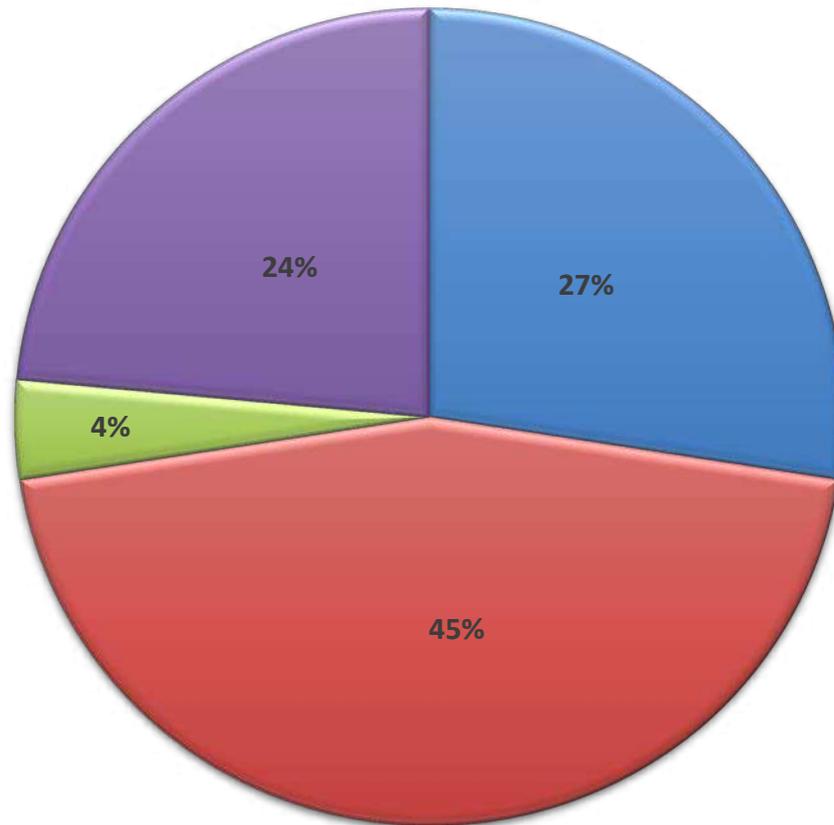
Top Findings
Contracted Noncriminal Justice Functions
Event Logging
Encryption
Personally Owned Information Systems
Media Disposal
Security Awareness Training
Security Audits
Physical Security



Breakdown Noncriminal Justice Agencies

Percentage of Event Logging OUTs

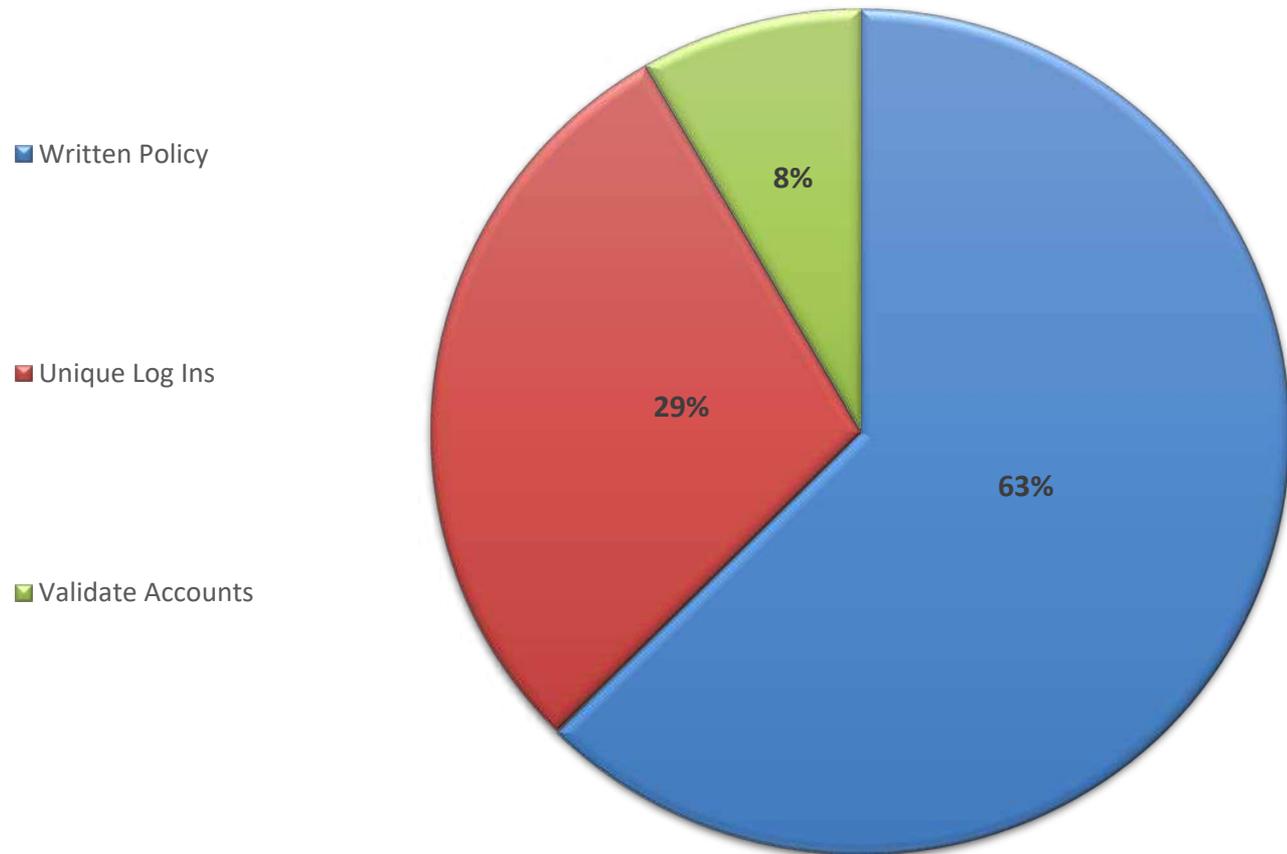
- No weekly review
- No logging/Not logging required events
- Logging failure does not provide alerts
- Log Rentention





Breakdown Noncriminal Justice Agencies

Percentage of Identification/UserID OUTs

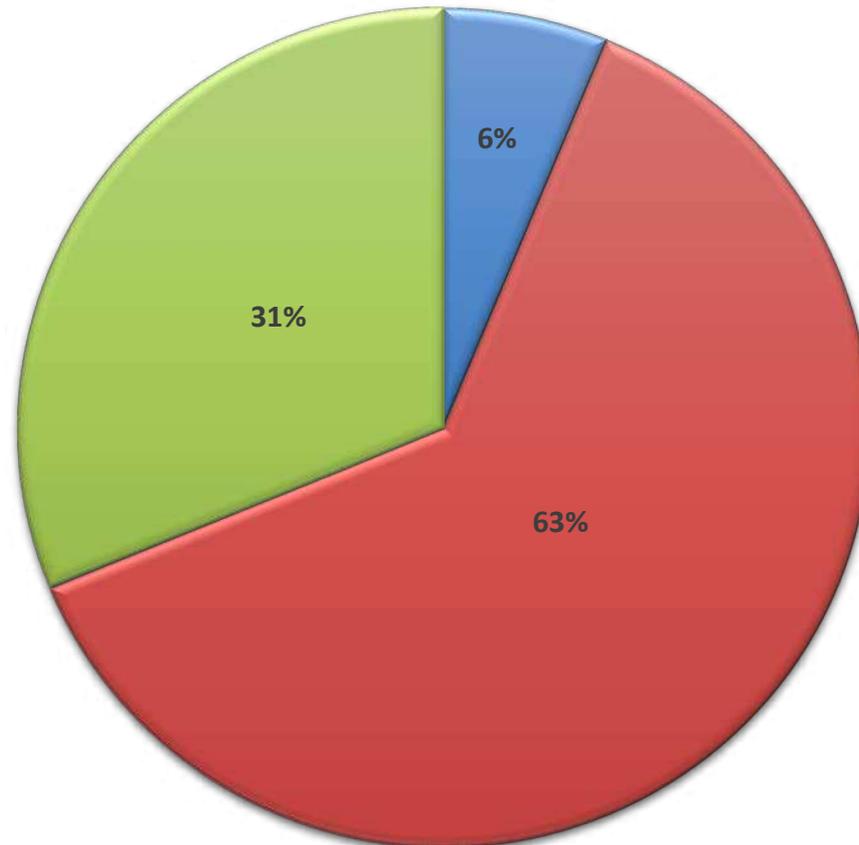




Breakdown Noncriminal Justice Agencies

Percentage of Media Disposal OUTs

- Release of Hard Drives without Wipe
(leased/rented copiers)
- Written Policy
- Physical Media Destruction not
witnessed by Authorized Personnel

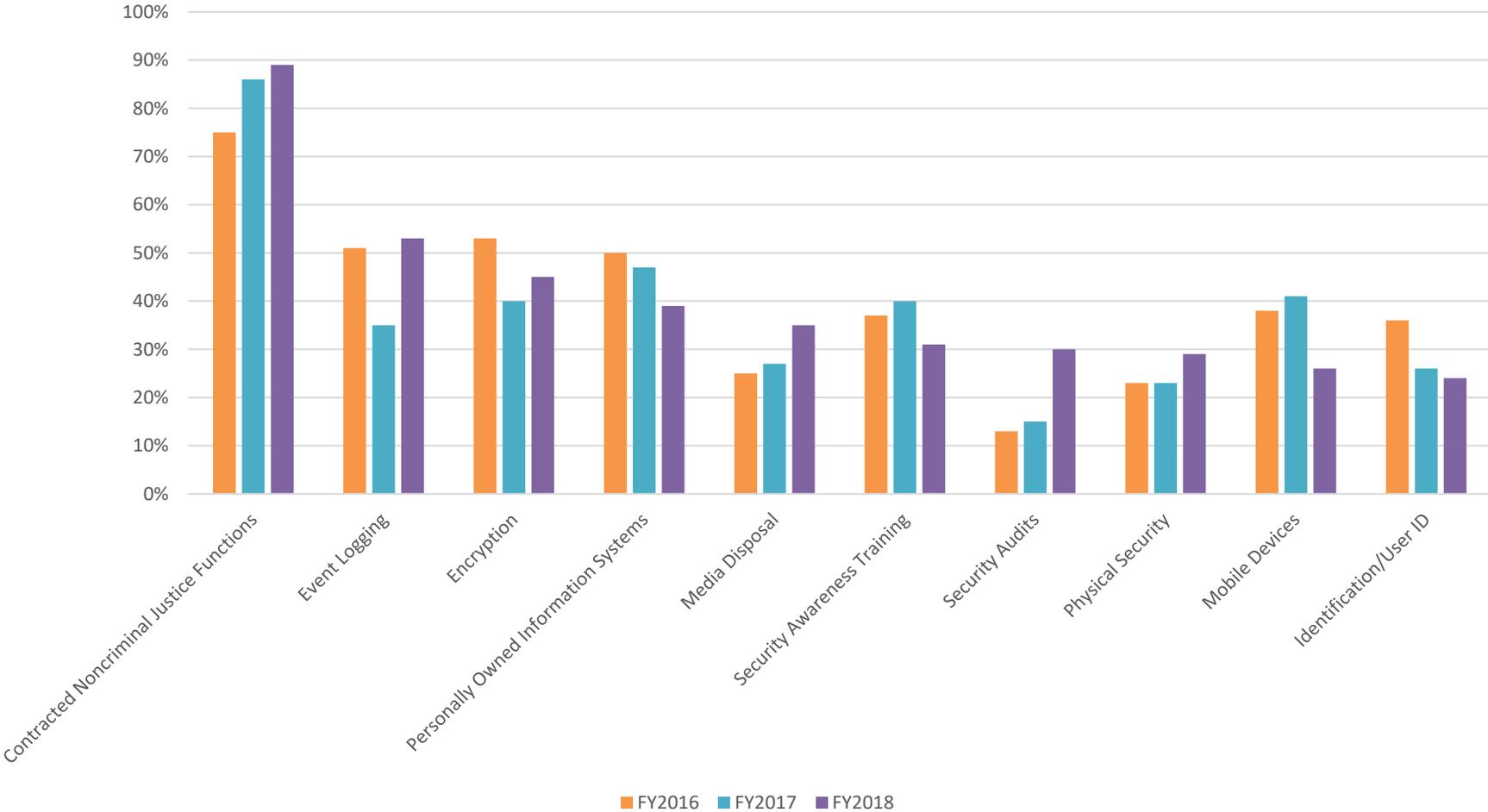




Noncriminal Justice Agency Trends



Noncriminal Justice Agency Trends





FY 2018



CJA Top Findings	NCJA Top Findings
Event Logging	Contracted Noncriminal Justice Functions
Encryption	Event Logging
Advanced Authentication	Encryption
Identification/UserID	Personally Owned Information Systems
System Use Notification	Media Disposal
Management Control Agreements	Security Awareness Training
Security Addendums	Security Audits
Security Awareness Training	Physical Security
Personally Owned Information Systems	Mobile Devices
Media Disposal	Identification/UserID



Repeat Offenders

Fiscal Year 2018



Top Findings at Both CJA and NCJA

Contractors (MCA/Security Addendum/Outsourcing)

Event Logging

Encryption

Personally Owned Information Systems (written policy)

Media Disposal

Security Awareness Training

Identification/UserID



What's New?

Assessment updates...

- MDM no longer assessed for indirect access systems
 - Still assessed for direct access from limited operating systems
- Private Contractor Agreements (5.1.1.5)
 - Only impacts Criminal Justice Functions/Criminal Justice Agency
 - Identifies the purpose and scope of providing services
 - Incorporates the *CJIS Security Policy*/CJIS Security Addendum



Questions



***Please address questions and
comments to:***

CJISAUDIT@fbi.gov



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:

- Replaced Disaster Recovery site for CJIS Object Store
- Stores fingerprints, mugshots, police reports, etc.

Size:

- 18 Billion objects
- 2.5 PB storage
- 300 new/updates per second

Obstacles Overcome:

- Hot migration of live system (servicing NGI and N-DEx)
- Replicated onsite objects over the wire while maintaining consistency of creates/updates/deletes

Benefits Realized:

- Refactored to leverage cloud-managed services (Oracle RDBMS replaced with DynamoDB and RDS)
- Dynamically scaled compute, storage, and database capacity
- Cloud services provided access to features not available on-premise



What We Migrated:

- Online Data Standards Website
- <https://datastandards.cjis.gov>

Size:

- ~10 servers

Obstacles Overcome:

- Engineering security stack (DMZ/AWS DirectConnect/VPC configuration/etc.) for a public website through the TIC

Benefits Realized:

- Less time and labor spent on capacity planning
- Less time and labor spent on logistics (hardware install/configuration)
- Increased efficiency in security assessments
- 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



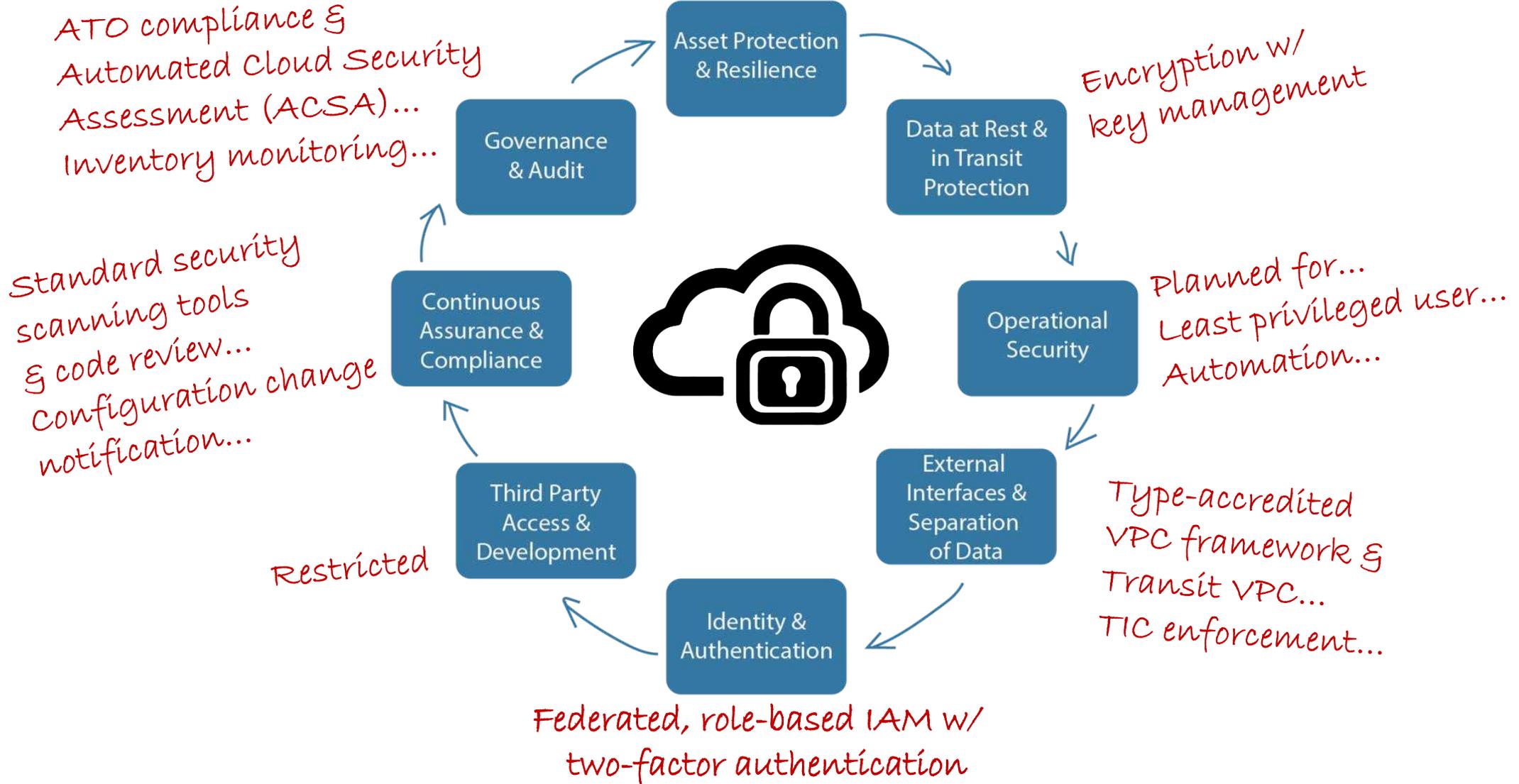
Migration planning
after successful proof
of concept for tactical
and offline searches



First phase of
functionality in Cloud
early next year



Design for resilience
FedRAMP Moderate/High only





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.