CJIS Security Policy

2018 FBI CJIS ISO Symposium

June 12 – 14, 2018

Jeff Campbell
FBI CJIS Deputy Information Security Officer

Discussion Topics

- Shared Management Philosophy
- Advisory Policy Board & Compact Council Overview
- CJIS Security Policy v5.6 Changes
- 2017 APB Topics (v5.7 Changes)
- ISO Resources

Shared Management Philosophy

Christine

Christine – ’58 Plymouth Fury

CJIS SECURITY POLICY SHARED MANAGEMENT PHILOSPHY

Where does criminal justice information (CJI) come from?

- State
- Local
- Tribal
- Federal

Because the information is shared…

- The FBI CJIS Division employs a shared management philosophy with state, local, tribal, and federal law enforcement agencies.

What does 'shared management' mean?

- Through the Advisory Policy Board process, the FBI along with state, local, tribal, and federal data providers and system users share responsibility for the protection of CJI and the operation and management of all systems administered by the CJIS Division for the benefit of the criminal justice community.

CJIS SECURITY POLICY SHARED MANAGEMENT PHILOSPHY

How does ‘shared management’ work?

- Designation of a CJIS Systems Agency (CSA)
- Designation of a CJIS Systems Officer (CSO)
- CJIS Advisory Process

The CJIS Advisory Process is used to…

- obtain the user community’s advice and guidance on the operation of all of the CJIS programs
- establish a minimum standard of requirements to ensure continuity of information protection (write minimum policy standards)
- represent the shared responsibility between the FBI CJIS, CJIS Systems Agency (CSA), and the State Identification Bureaus (SIB) of the lawful use and appropriate protection of CJI

CJIS SECURITY POLICY SHARED MANAGEMENT PHILOSPHY

Risk-based Approach to Compliance with the CJIS Security Policy

- Executive Summary:

  “The Policy empowers CSAs with the insight and ability to tune their security programs according to their risks, needs, budgets, and resource constraints while remaining compliant with the baseline level of security set forth in this Policy.”

- Section 2.3 Risk Versus Realism:

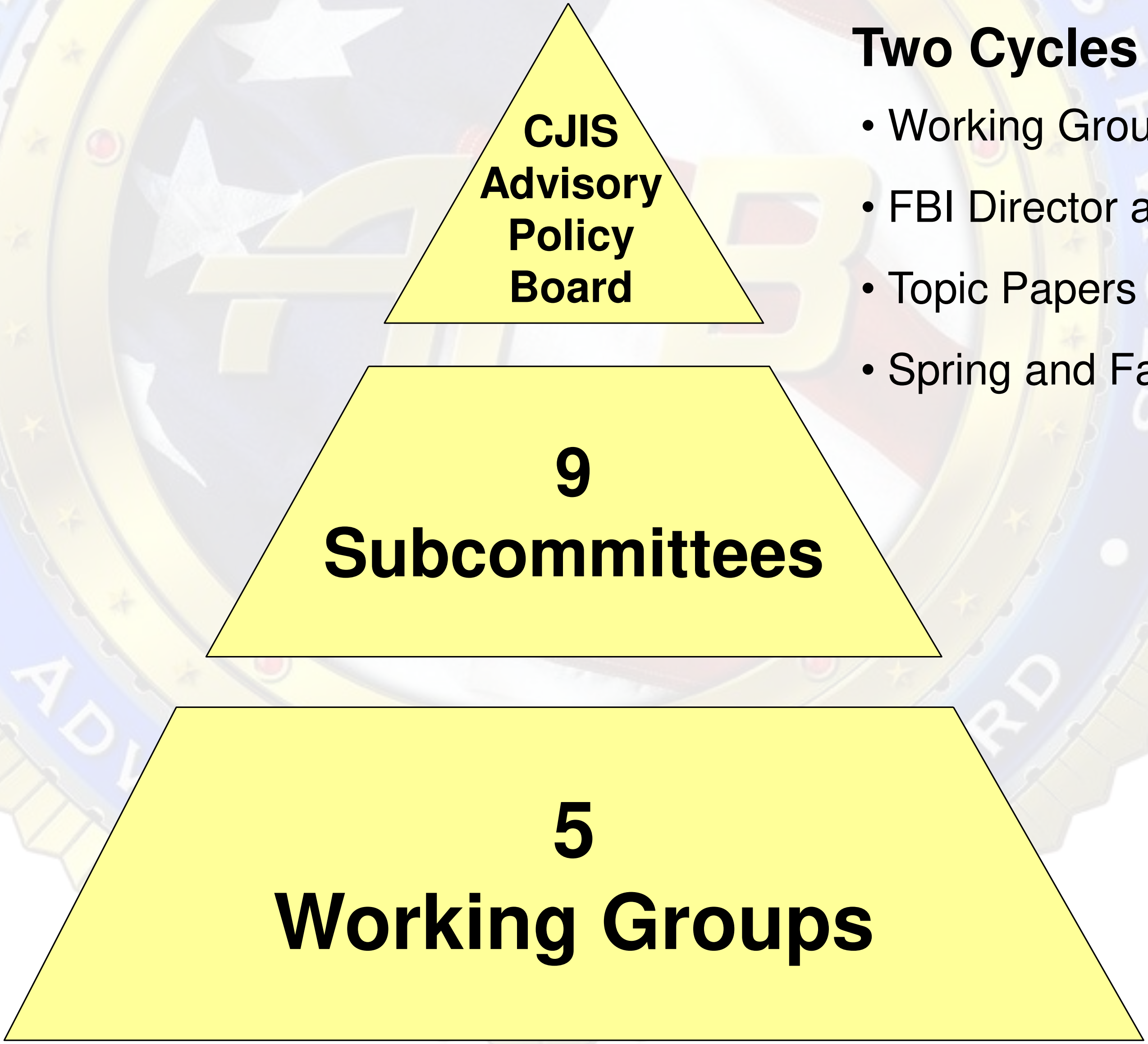
  “Each agency faces risk unique to that agency. It is quite possible that several agencies could encounter the same type of risk however depending on resources would mitigate that risk differently. In that light, a risk-based approach can be used when implementing requirements.”

Advisory Policy & Compact

Overview

Gone in 60 Seconds
Eleanor – ’67 Ford Mustang Shelby GT500

CJIS ADVISORY PROCESS



CJIS Advisory Policy Board

9 Subcommittees

5 Working Groups

Two Cycles Annually

- Working Groups, Subcommittees, Board
- FBI Director approval
- Topic Papers
- Spring and Fall

CJIS ADVISORY PROCESS

WHAT DO THE WORKING GROUPS (WGs) DO?

- Review operational, policy, and technical issues related to CJIS Division programs and policies and make recommendations to the APB or one of the subcommittees

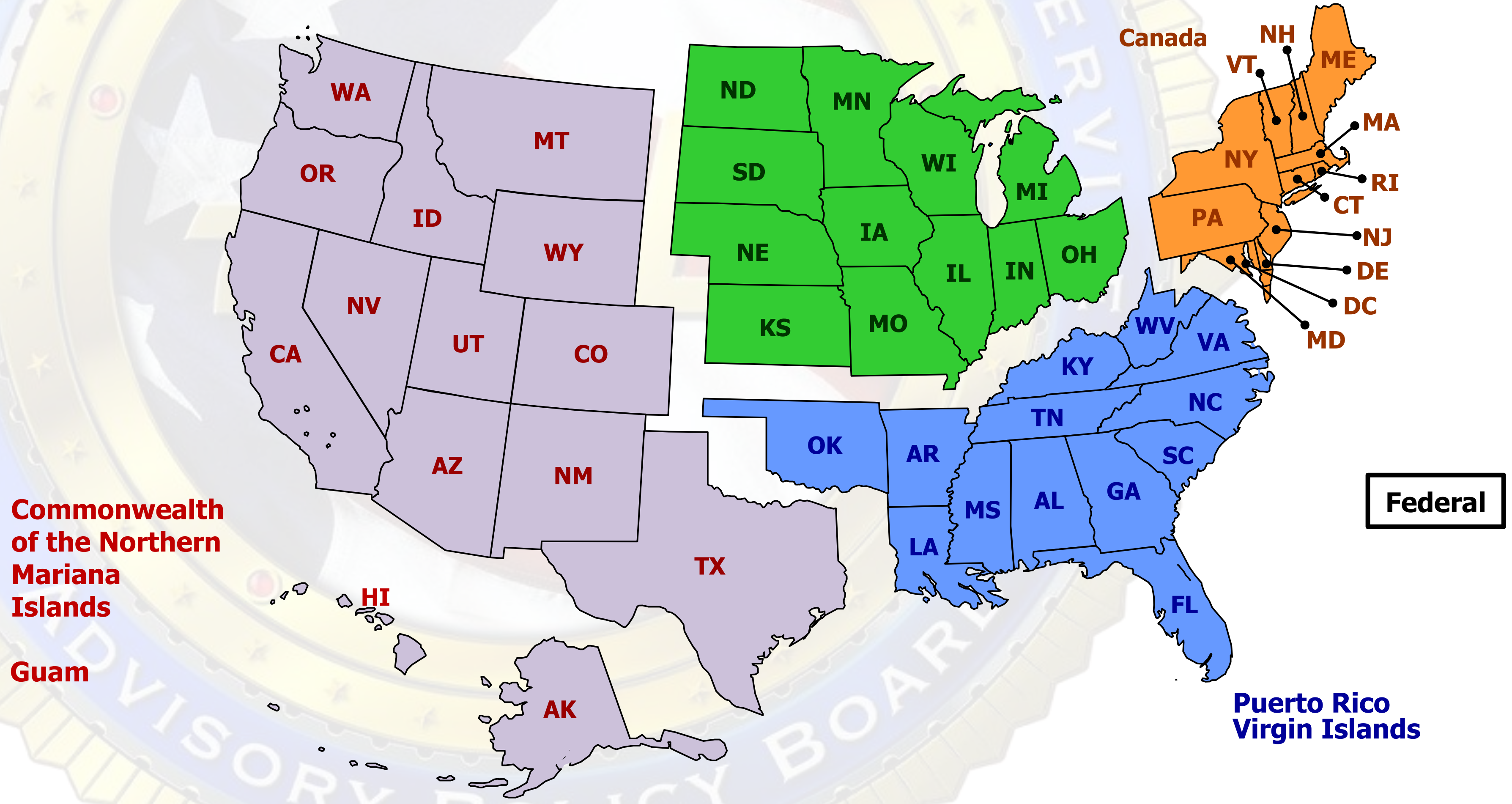
- All 50 states, as well as U.S. territories and the Royal Canadian Mounted Police (RCMP) – Canadian Police Information Centre (CPIC) are organized into four Regional Working Groups: Northeastern, North Central, Southern and Western

- The four regional WGs are composed of:
  - One state-level agency representative selected by the Administrator of each states CJIS System Agency (CSA)
  - One local-level agency representative selected by the International Association of Chiefs of Police (IACP) or National Sheriffs' Association (NSA) along with State Chiefs' or Sheriffs' Association
  - One representative for the District of Columbia, Guam, Commonwealth of the Northern Mariana Islands (CNMI), RCMP, Puerto Rico, and the U. S. Virgin Islands
  - One Tribal law enforcement representative for each region.

- The FBI Director may designate one additional representative for each 5 WGs.

CJIS ADVISORY PROCESS

Advisory Policy Board Working Group Regions



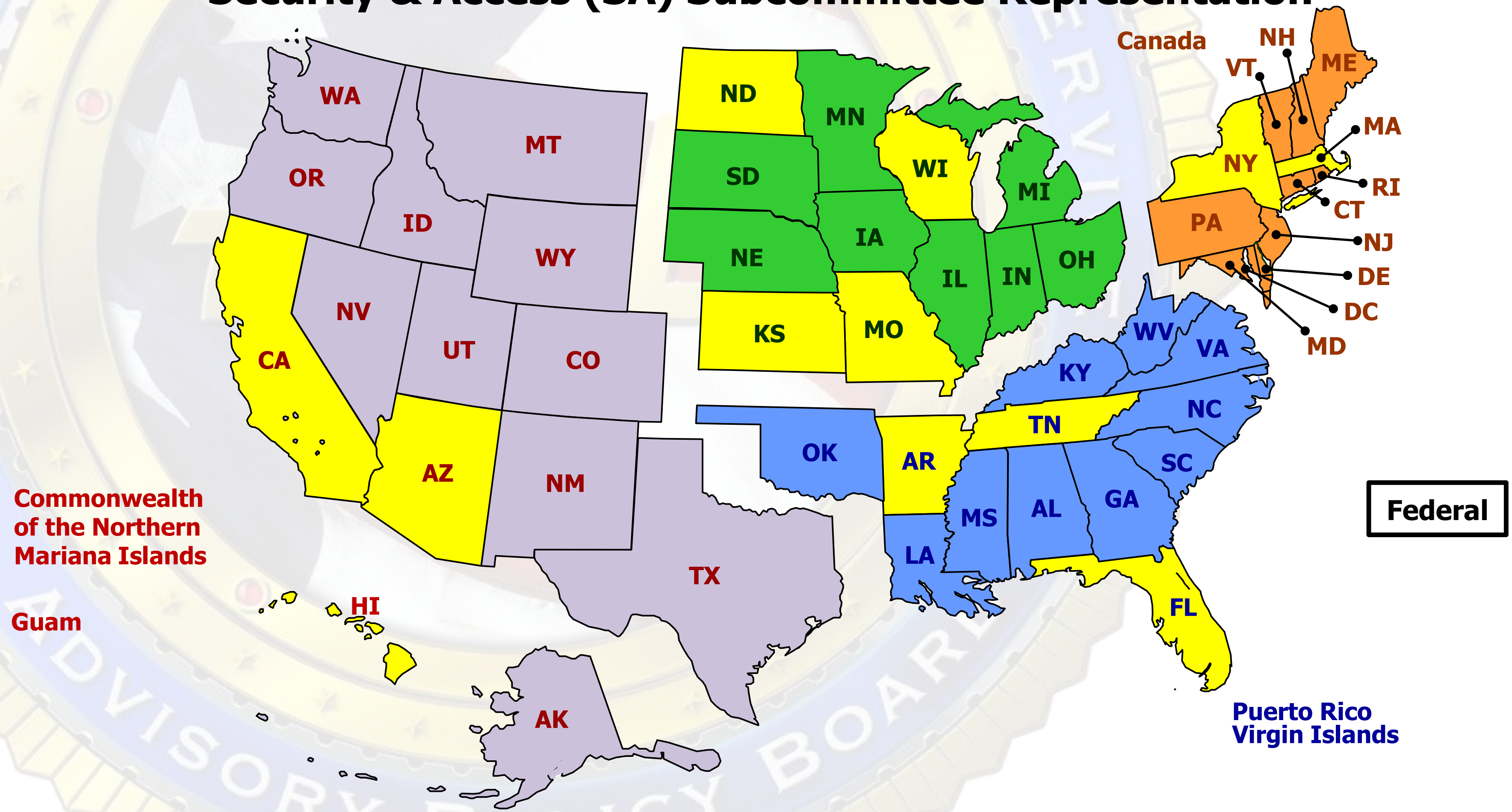
CJIS ADVISORY PROCESS

NINE SUBCOMMITTEES:

- Uniform Crime Reporting (UCR)
- APB Executive Committee
- Compliance Evaluation (formerly Sanctions)
- National Crime Information Center (NCIC)
- Identification Services (IS)
- N-DEx (formerly Information Sharing)
- **Security and Access (SA)**
- National Instant Criminal Background Check System (NICS)
- Bylaws

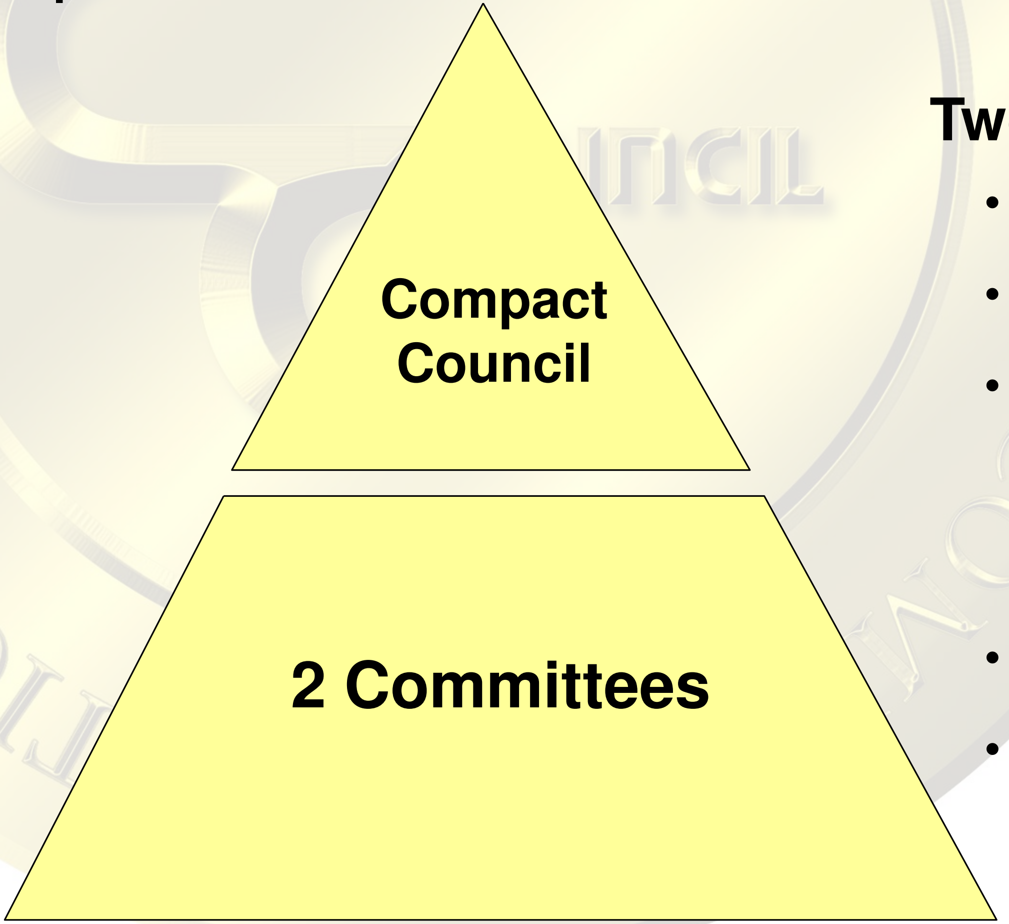
CJIS ADVISORY PROCESS

Security & Access (SA) Subcommittee Representation



COMPACT COUNCIL

NATIONAL CRIME PREVENTION AND PRIVACY COMPACT COUNCIL –
Est. October 8, 1998, provides Federal Authority for the interstate exchange of state criminal history record information (CHRI) for noncriminal justice purposes.

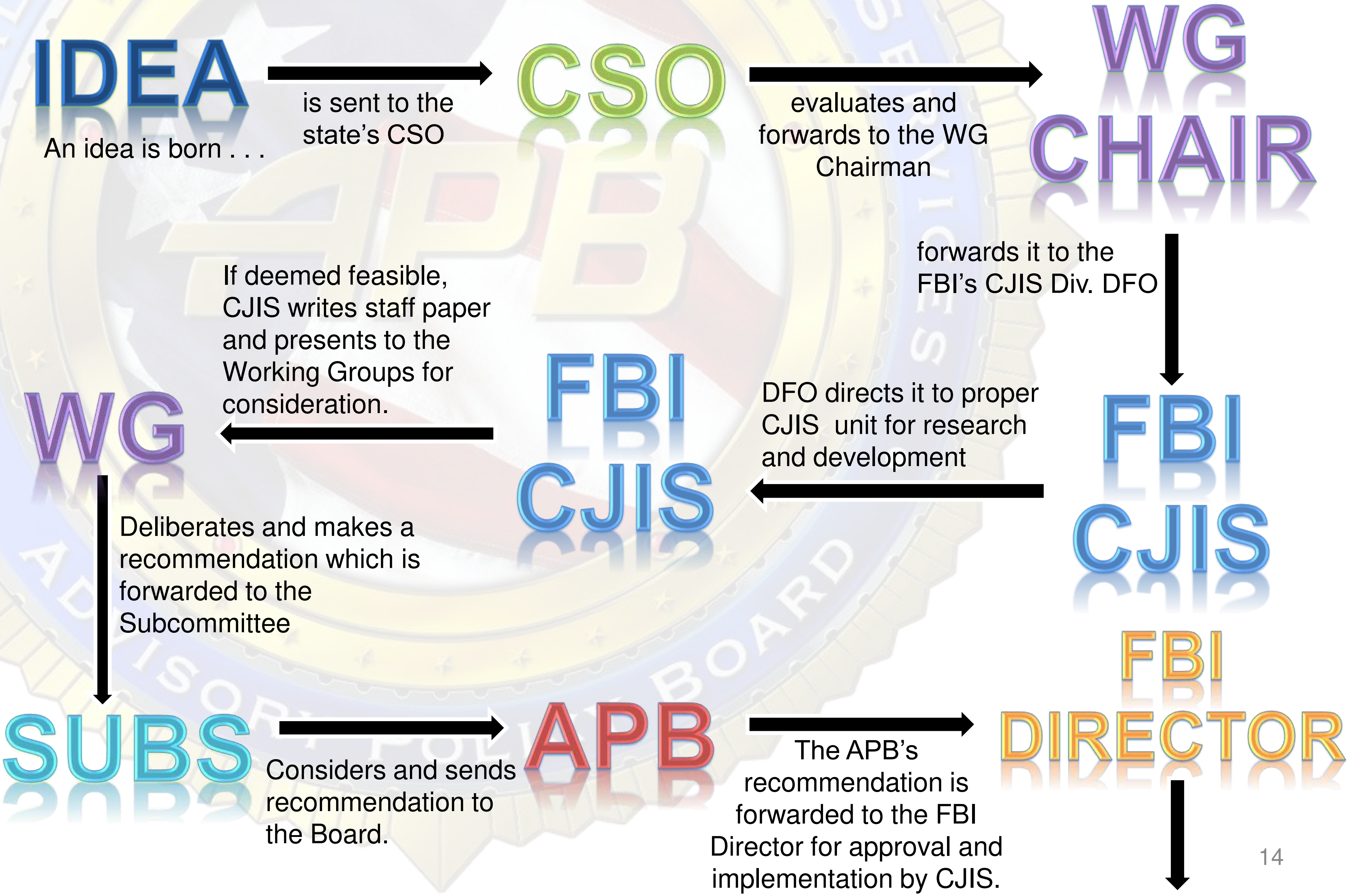


Two Cycles Annually

- Spring and Fall
- Committees, Council
- Topic Papers

- Standards & Policy
- Planning & Outreach

CJIS ADVISORY PROCESS



IDEA

An idea is born . . .

is sent to the state's CSO

CSO

evaluates and forwards to the WG Chairman

WG CHAIR

forwards it to the FBI's CJIS Div. DFO

FBI CJIS

DFO directs it to proper CJIS unit for research and development

FBI CJIS

If deemed feasible, CJIS writes staff paper and presents to the Working Groups for consideration.

WG

Deliberates and makes a recommendation which is forwarded to the Subcommittee

SUBS

Considers and sends recommendation to the Board.

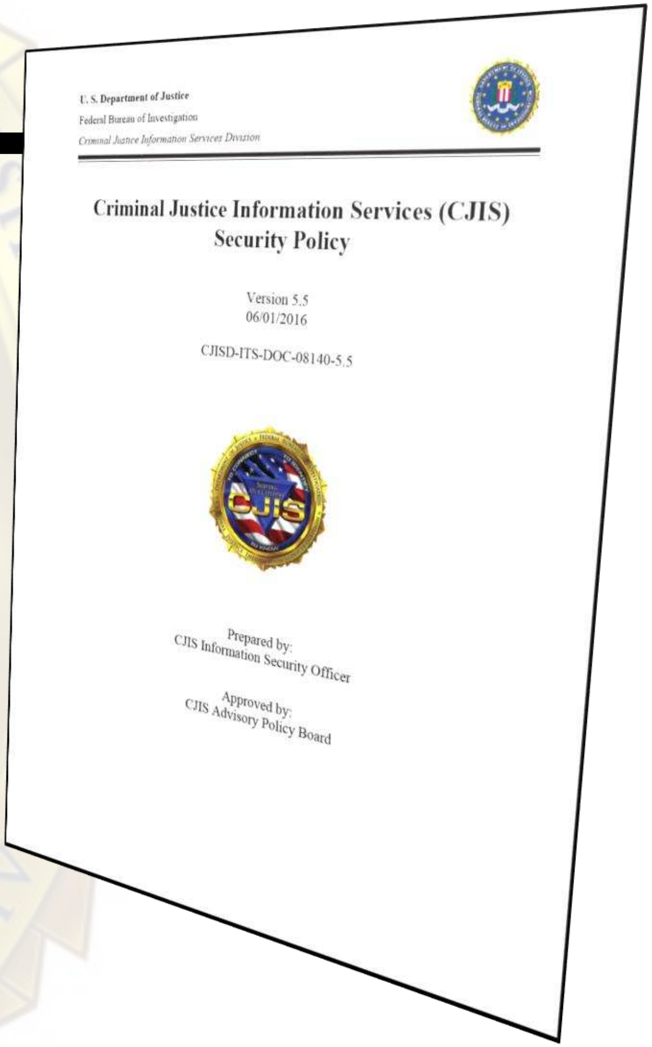
APB

The APB's recommendation is forwarded to the FBI Director for approval and implementation by CJIS.

FBI DIRECTOR

CJIS SECURITY POLICY

- □ Minimum requirements for the protection of criminal justice information (CJI)
- □ Annual release cycle
- □ Early Summer Time Frame
- □ Incorporates APB approved changes from previous year (2 cycles: Spring / Fall)
- □ Incorporates administrative changes



U. S. Department of Justice
Federal Bureau of Investigation
Criminal Justice Information Services Division

Criminal Justice Information Services (CJIS)
Security Policy

Version 5.5
06/01/2016

CJISD-ITS-DOC-08140-5.5

Prepared by:
CJIS Information Security Officer

Approved by:
CJIS Advisory Policy Board

CJIS Security Policy

v5.6 Changes

Smokey and the Bandit
Bandit – ’77 Pontiac Trans Am

NEW CHANGES IN v5.6

Policy Area 6: Identification and Authentication

Section 5.6.2.1 Standard Authenticators

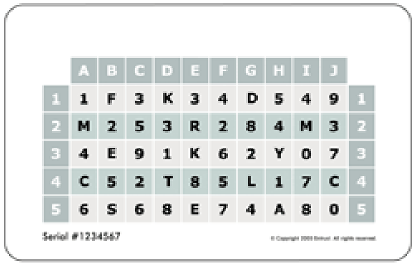
“Authenticators are (the something you know, something you are, or something you have) part of the identification and authentication process. Examples of standard authenticators include passwords, ***hard or soft*** tokens, biometrics, ***one-time passwords (OTP)*** and personal identification numbers (PIN). Users…”

NEW CHANGES IN v5.6

Policy Area 6: Identification and Authentication

Section 5.6.2.1.3 One-time Passwords (OTP)

One-time passwords are considered a "something you have" token for authentication. Examples include bingo cards, hard or soft tokens, and out-of-band tokens (i.e. OTP received via a text message).



	A	B	C	D	E	F	G	H	I	J	
1	1	F	3	K	3	4	D	5	4	9	1
2	M	2	5	3	R	2	8	4	M	3	2
3	4	E	9	1	K	6	2	Y	0	7	3
4	C	5	2	T	8	5	L	1	7	C	4
5	6	S	6	8	E	7	4	A	8	0	5

Serial #1234567

© Copyright 2005 Entrust. All rights reserved.

NEW CHANGES IN v5.6

Policy Area 6: Identification and Authentication

Section 5.6.2.1.3 One-time Passwords (OTP)

When agencies implement the use of an OTP as an authenticator, the OTP shall meet the requirements described below.

- ***a. Be a minimum of six (6) randomly generated characters***
- ***b. Be valid for a single session***
- ***c. If not used, expire within a maximum of five (5) minutes after issuance***

NEW CHANGES IN v5.6

Policy Area 10: System and Communications Protection and Information Integrity

Section 5.10.1.2 Encryption

Revamped the section, read my lips: NO NEW REQUIREMENTS!

Separate sections for:

- 5.10.1.2.1 Encryption for CJI in Transit
- 5.10.1.2.2 Encryption for CJI at Rest
- 5.10.1.2.3 Public Key Infrastructure

No requirement changes:

- CJI in transit is still FIPS 140-2 certified, 128 bit symmetric
- CJI at rest can be FIPS 140-2 certified, 128 bit symmetric or FIPS 197 (AES), 256 bit symmetric

NEW CHANGES IN v5.6

Policy Area 11: Formal Audits

Section 5.11.4 Compliance Subcommittees

Paragraphs describing compliance subcommittees and their function in respective processes

- APB – Compliance Evaluation Subcommittee
    - Evaluate audit results
    - Provide recommendations for compliance
- Compact – Compact Council Sanctions Committee
    - Ensure use of III for noncriminal justice purposes is compliant
    - Review audit results and participant's response
    - Determine course of action for compliance
    - Provide recommendations

NEW CHANGES IN v5.6

Appendices

Appendix A: Terms and Definitions

New Definitions:

- Asymmetric Encryption
- Decryption
- Encryption
- Hybrid Encryption
- Symmetric Encryption

Appendix G: Best Practices

New Best Practice:

- G.6 Encryption
  - Symmetric vs. Asymmetric comparison
  - FIPS 140-2 explanation
  - General Recommendations

CJIS Security Policy

2017 APB Topics

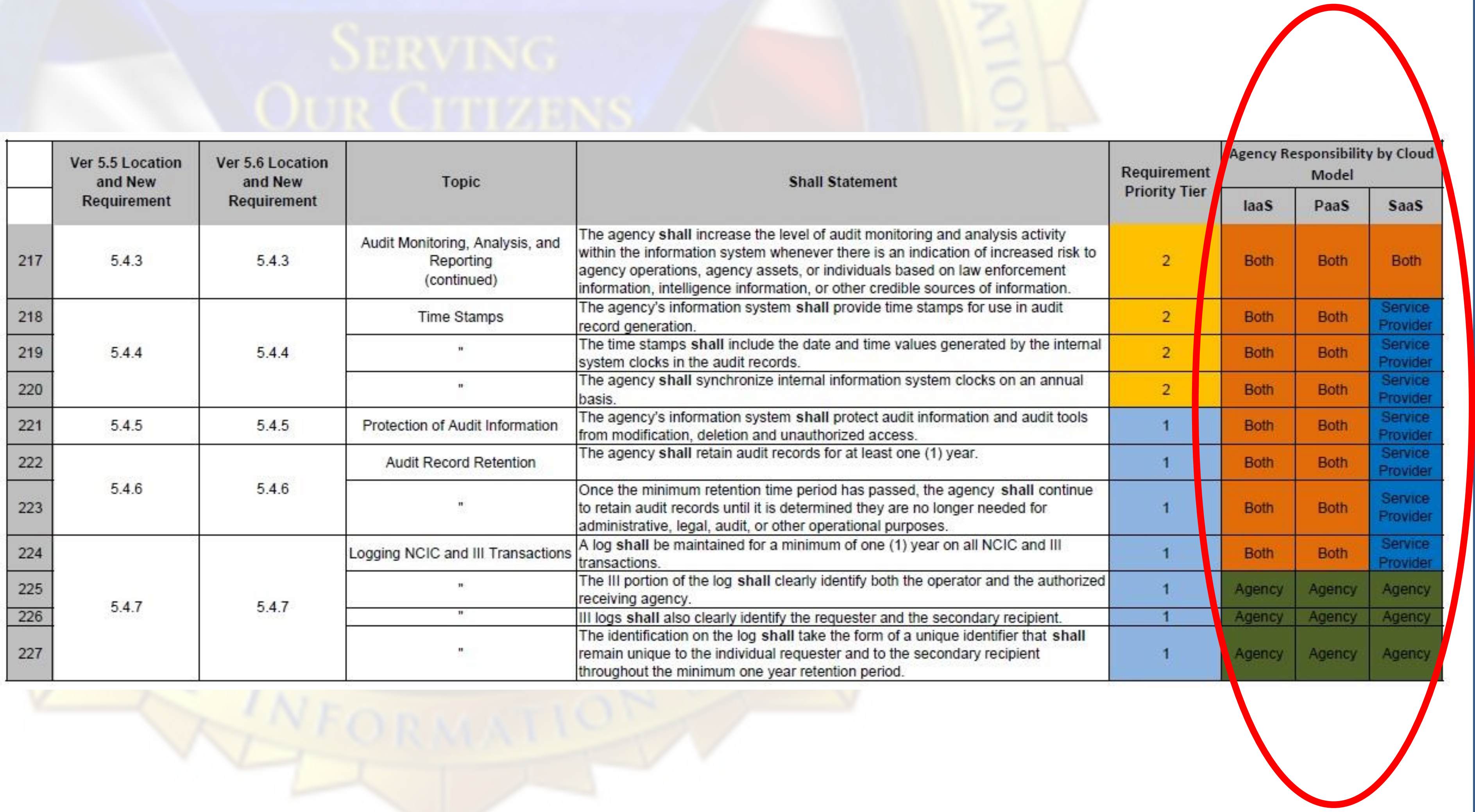
Batman: The Movie
Batmobile – ’54 Lincoln Futura

CJIS SECURITY POLICY OVERVIEW

Spring 2017 APB Topics

- **CSO Latitude for non-felony background results on contractors – approved**
- **Cloud metadata use – approved**
- **Off-shore storage of data – fall**
- **MDM awareness – info only**
- **ISO Annual Update – info only**
- **CJIS Security Policy Companion Document – info only**

CJIS SECURITY POLICY OVERVIEW



	Ver 5.5 Location and New Requirement	Ver 5.6 Location and New Requirement	Topic	Shall Statement	Requirement Priority Tier	Agency Responsibility by Cloud Model		
						IaaS	PaaS	SaaS
217	5.4.3	5.4.3	Audit Monitoring, Analysis, and Reporting (continued)	The agency **shall** increase the level of audit monitoring and analysis activity within the information system whenever there is an indication of increased risk to agency operations, agency assets, or individuals based on law enforcement information, intelligence information, or other credible sources of information.	2	Both	Both	Both
218	5.4.4	5.4.4	Time Stamps	The agency's information system **shall** provide time stamps for use in audit record generation.	2	Both	Both	Service Provider
219			"	The time stamps **shall** include the date and time values generated by the internal system clocks in the audit records.	2	Both	Both	Service Provider
220			"	The agency **shall** synchronize internal information system clocks on an annual basis.	2	Both	Both	Service Provider
221	5.4.5	5.4.5	Protection of Audit Information	The agency's information system **shall** protect audit information and audit tools from modification, deletion and unauthorized access.	1	Both	Both	Service Provider
222	5.4.6	5.4.6	Audit Record Retention	The agency **shall** retain audit records for at least one (1) year.	1	Both	Both	Service Provider
223			"	Once the minimum retention time period has passed, the agency **shall** continue to retain audit records until it is determined they are no longer needed for administrative, legal, audit, or other operational purposes.	1	Both	Both	Service Provider
224	5.4.7	5.4.7	Logging NCIC and III Transactions	A log **shall** be maintained for a minimum of one (1) year on all NCIC and III transactions.	1	Both	Both	Service Provider
225			"	The III portion of the log **shall** clearly identify both the operator and the authorized receiving agency.	1	Agency	Agency	Agency
226			"	III logs **shall** also clearly identify the requester and the secondary recipient.	1	Agency	Agency	Agency
227			"	The identification on the log **shall** take the form of a unique identifier that **shall** remain unique to the individual requester and to the secondary recipient throughout the minimum one year retention period.	1	Agency	Agency	Agency

Fall 2017 APB Topics

- Restriction of off-shore storage of data – approved
- Vetting of non-resident, non-U.S. citizens – OBE
- Section 5.12 changes – approved

Section 5.12 Personnel Security Change Highlights

- “Unescorted access to unencrypted CJI”
- Fingerprint-based background check required before gaining access to CJI
- Felony for contractor/vendor no longer automatic disqualifier

FBI CJIS ISO Resources

Bullitt
‘68 Ford Mustang GT 390

ISO RESOURCES

CJIS ISO Program

- Steward the CJIS Security Policy for the Advisory Policy Board
  - Draft and present topic papers at the APB meetings
- Provide Policy support to state ISOs and CSOs
  - Policy Clarification
  - Solution technical analysis for compliance with the Policy
  - Operate a public facing web site on FBI.gov: CJIS Security Policy Resource Center
- Provide training support to ISOs
- Provide policy clarification to vendors in coordination with ISOs

iso@fbi.gov

ISO RESOURCES

CJIS Security Policy Requirements Companion Document

- Companion document to the CJIS Security Policy
- Lists every requirement, “shall” statement, and corresponding location and effective date
- Lists the priority tier (1 or 2) for each requirement
- Cloud “matrix” which shows the technical capability to meet requirements
- Updated annually in conjunction with the CJIS Security Policy

iso@fbi.gov

ISO RESOURCES

CJIS Security Policy Mapping to NIST 800-53 rev 4

- Auxiliary document to the CJIS Security Policy
- Maps Policy sections to related NIST SP800-53r4 controls
  - Moderate impact level controls plus some related controls
- Technical assessments for federal systems require the use of NIST controls for compliance evaluation (e.g. FISMA, FedRAMP)
- Not all Policy requirements map to NIST controls
  - Policy requirements originate from 28 CFR
  - Policy requirements unique to CJI

iso@fbi.gov

ISO RESOURCES

CJIS Security Policy Resource Center

- ❑ Publically Available:

  http://www.fbi.gov/about-us/cjis/cjis-security-policy-resource-center/view

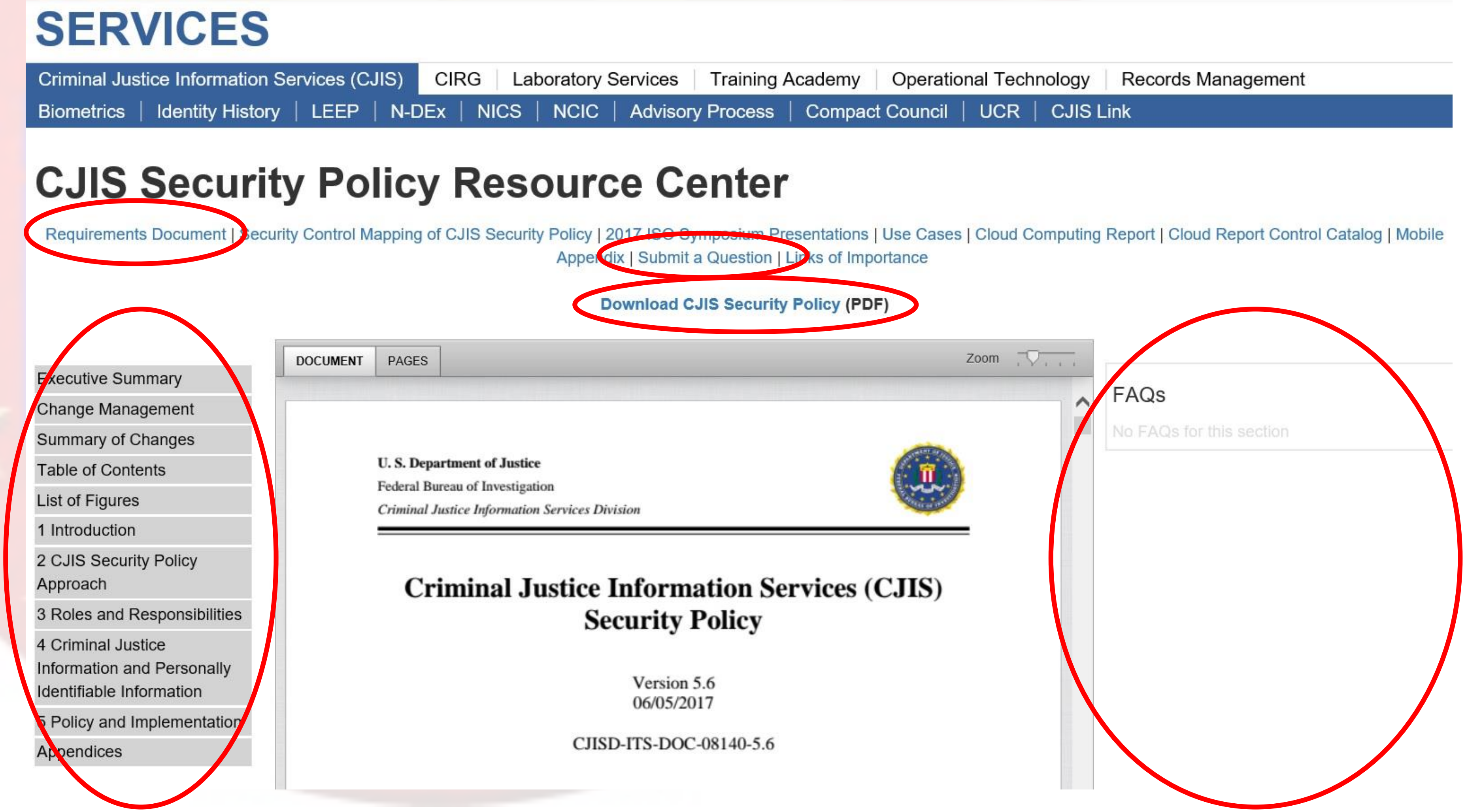
- ❑ Features:
  - Search and download the CJIS Security Policy
  - Download the CJIS Security Policy Requirements and Tiering Document
  - Use Cases (Advanced Authentication and others to follow)
  - Cloud Computing Report & Cloud Report Control Catalog
  - Mobile Appendix
  - Submit a Question (question forwarded to CJIS ISO Program)
  - Links of importance

iso@fbi.gov

ISO RESOURCES

CJIS Security Policy Resource Center

http://www.fbi.gov/about-us/cjis/cjis-security-policy-resource-center/view



SERVICES
Criminal Justice Information Services (CJIS) | CIRG | Laboratory Services | Training Academy | Operational Technology | Records Management
Biometrics | Identity History | LEEP | N-DEx | NICS | NCIC | Advisory Process | Compact Council | UCR | CJIS Link

CJIS Security Policy Resource Center

Requirements Document | Security Control Mapping of CJIS Security Policy | 2017 ISO Symposium Presentations | Use Cases | Cloud Computing Report | Cloud Report Control Catalog | Mobile Appendix | Submit a Question | Links of Importance

Download CJIS Security Policy **(PDF)**

- Executive Summary
- Change Management
- Summary of Changes
- Table of Contents
- List of Figures
- 1 Introduction
- 2 CJIS Security Policy Approach
- 3 Roles and Responsibilities
- 4 Criminal Justice Information and Personally Identifiable Information
- 5 Policy and Implementation
- Appendices

U. S. Department of Justice
Federal Bureau of Investigation
Criminal Justice Information Services Division

Criminal Justice Information Services (CJIS) Security Policy

Version 5.6
06/05/2017

CJISD-ITS-DOC-08140-5.6

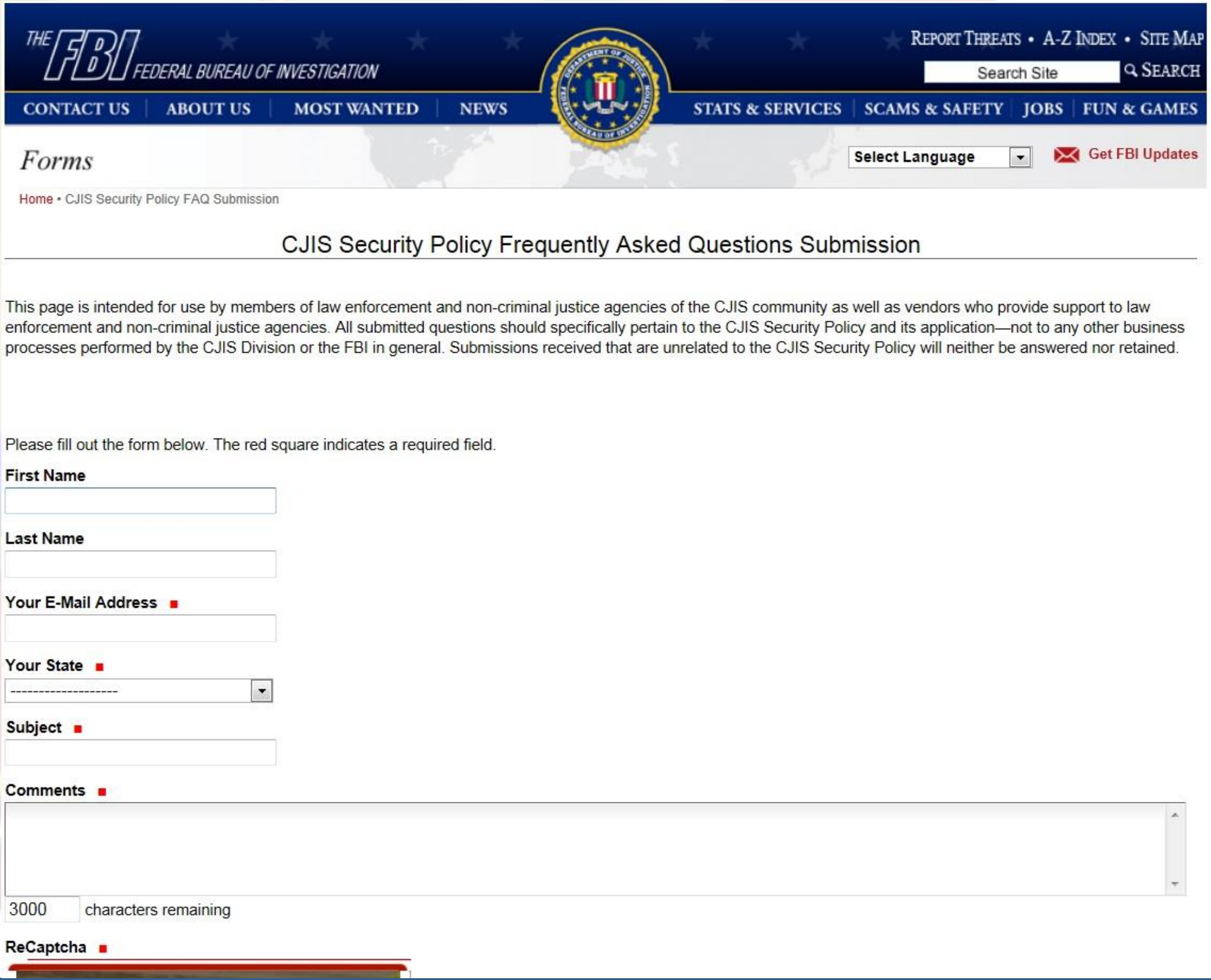
FAQs

No FAQs for this section

ISO RESOURCES

CJIS Security Policy Resource Center

http://www.fbi.gov/about-us/cjis/cjis-security-policy-resource-center/view



CJIS Security Policy Frequently Asked Questions Submission

This page is intended for use by members of law enforcement and non-criminal justice agencies of the CJIS community as well as vendors who provide support to law enforcement and non-criminal justice agencies. All submitted questions should specifically pertain to the CJIS Security Policy and its application—not to any other business processes performed by the CJIS Division or the FBI in general. Submissions received that are unrelated to the CJIS Security Policy will neither be answered nor retained.

Please fill out the form below. The red square indicates a required field.

First Name

Last Name

Your E-Mail Address ■

Your State ■

Subject ■

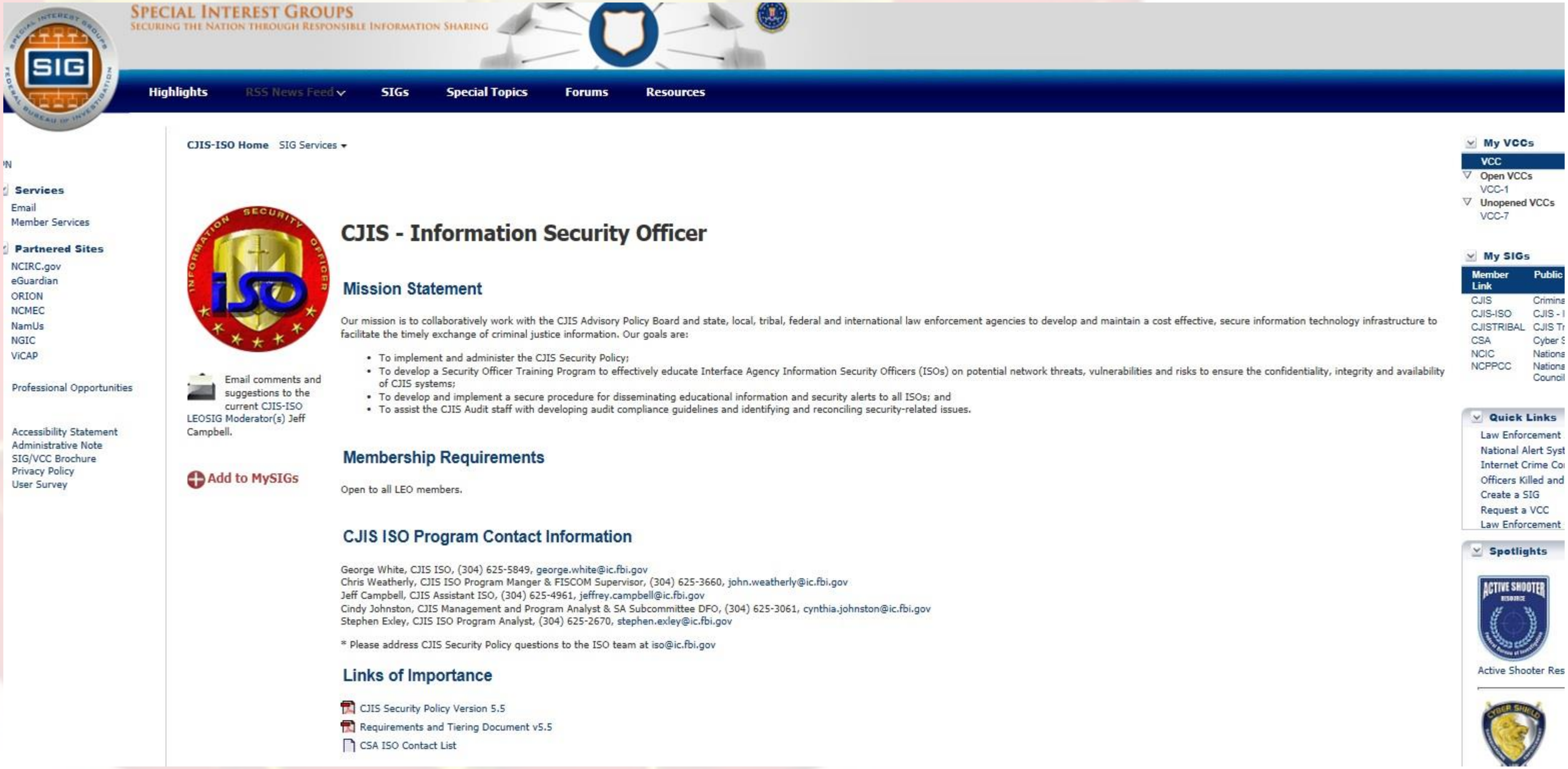
Comments ■

3000 characters remaining

ReCaptcha ■

ISO RESOURCES

CJIS Information Security Officer LEEP SIG



Email comments and suggestions to the current CJIS-ISO LEOSIG Moderator(s) Jeff Campbell.

CJIS - Information Security Officer

Mission Statement

Our mission is to collaboratively work with the CJIS Advisory Policy Board and state, local, tribal, federal and international law enforcement agencies to develop and maintain a cost effective, secure information technology infrastructure to facilitate the timely exchange of criminal justice information. Our goals are:

- To implement and administer the CJIS Security Policy;
- To develop a Security Officer Training Program to effectively educate Interface Agency Information Security Officers (ISOs) on potential network threats, vulnerabilities and risks to ensure the confidentiality, integrity and availability of CJIS systems;
- To develop and implement a secure procedure for disseminating educational information and security alerts to all ISOs; and
- To assist the CJIS Audit staff with developing audit compliance guidelines and identifying and reconciling security-related issues.

Membership Requirements

Open to all LEO members.

CJIS ISO Program Contact Information

George White, CJIS ISO, (304) 625-5849, george.white@ic.fbi.gov
Chris Weatherly, CJIS ISO Program Manger & FISCOM Supervisor, (304) 625-3660, john.weatherly@ic.fbi.gov
Jeff Campbell, CJIS Assistant ISO, (304) 625-4961, jeffrey.campbell@ic.fbi.gov
Cindy Johnston, CJIS Management and Program Analyst & SA Subcommittee DFO, (304) 625-3061, cynthia.johnston@ic.fbi.gov
Stephen Exley, CJIS ISO Program Analyst, (304) 625-2670, stephen.exley@ic.fbi.gov

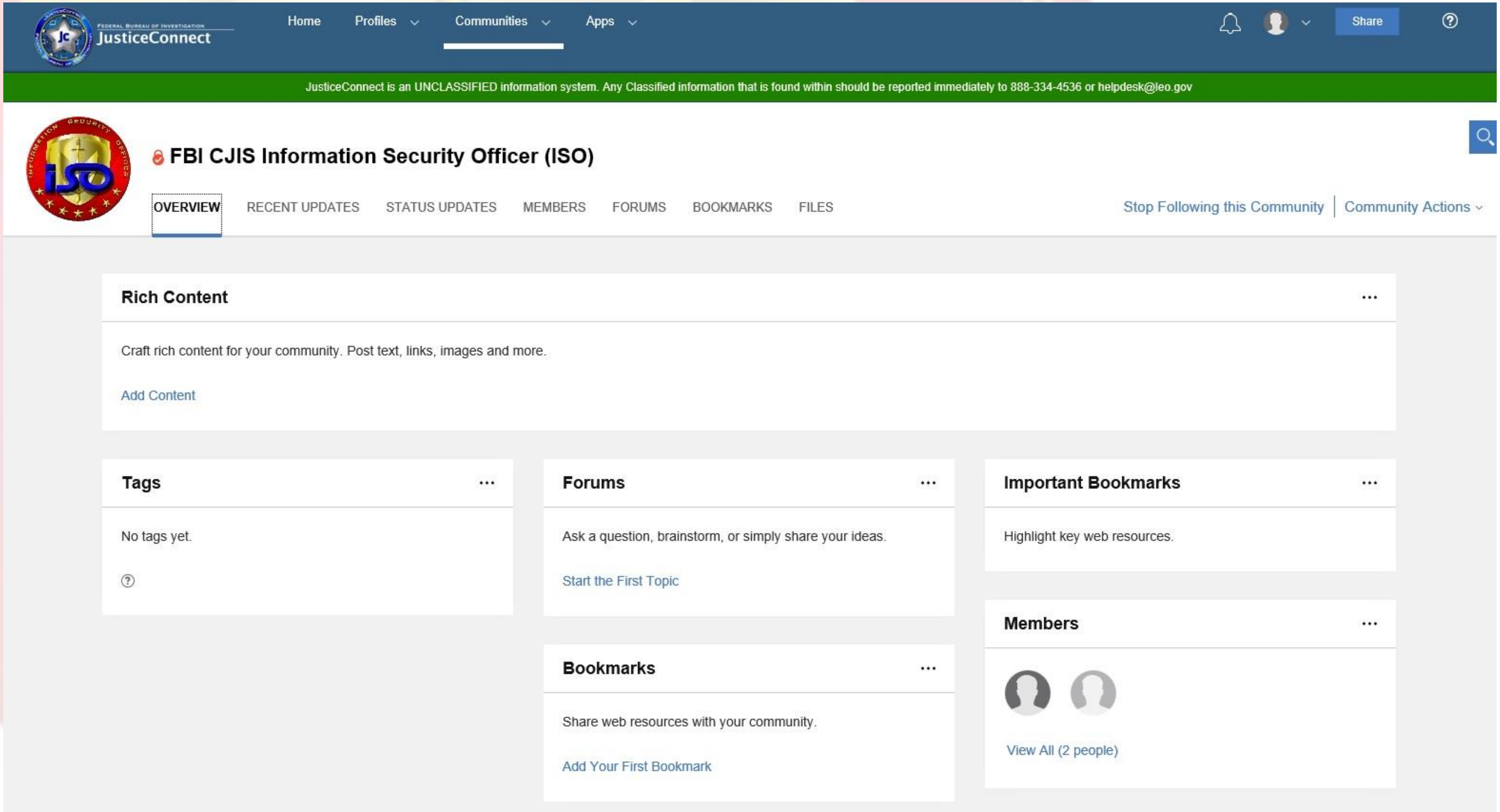
* Please address CJIS Security Policy questions to the ISO team at iso@ic.fbi.gov

Links of Importance

- CJIS Security Policy Version 5.5
- Requirements and Tiering Document v5.5
- CSA ISO Contact List

ISO RESOURCES

CJIS Information Security Officer Community



JusticeConnect is an UNCLASSIFIED information system. Any Classified information that is found within should be reported immediately to 888-334-4536 or helpdesk@leo.gov

FBI CJIS Information Security Officer (ISO)

Rich Content

Craft rich content for your community. Post text, links, images and more.

Add Content

Tags

No tags yet.

Forums

Ask a question, brainstorm, or simply share your ideas.

Start the First Topic

Important Bookmarks

Highlight key web resources.

Members

View All (2 people)

Bookmarks

Share web resources with your community.

Add Your First Bookmark

CJIS ISO CONTACT INFORMATION

Chris Weatherly FBI CJIS ISO	(304) 625 - 3660 jcweatherly@fbi.gov
Jeff Campbell FBI CJIS Deputy ISO	(304) 625 - 4961 jbcampbell@fbi.gov

iso@fbi.gov

Pathfinder to a: Hybrid Cloud Solution

GEORGE A. WHITE –CJIS INFORMATION ASSURANCE UNIT CHIEF

2014 Business Needs Projections: FY 2016-2018

- Technical refresh required for NGI HW and storage
- Initial estimate of XX-XX million dollars over 3 years
- FY 2016-2018 Constraints:
    - Cost estimates not supported by budget projections
    - Cloud-first executive order
    - FedRAMP High IaaS in progress

Mid-2016 Path

□Tech Refresh on-prem with commodity hardware

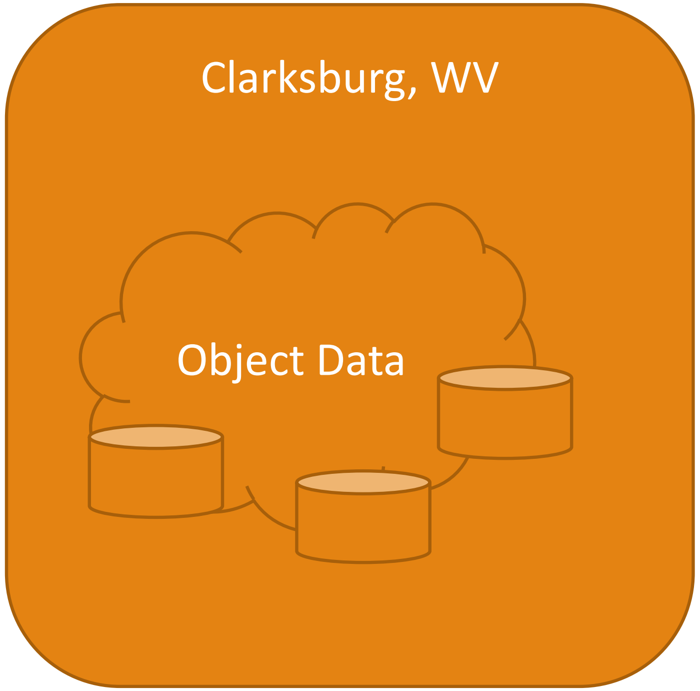
□ Pathfinder Cloud Services built by CJIS must also support the greater FBI unclassified needs

□Move Object Data Stored at PITC to Cloud

Object data is: A generic storage system where CJIS houses:

- ➢All biometric data
- ➢All Criminal History Messages
- ➢Various N-DEx data holdings (incident reports, entity relationship information, etc)

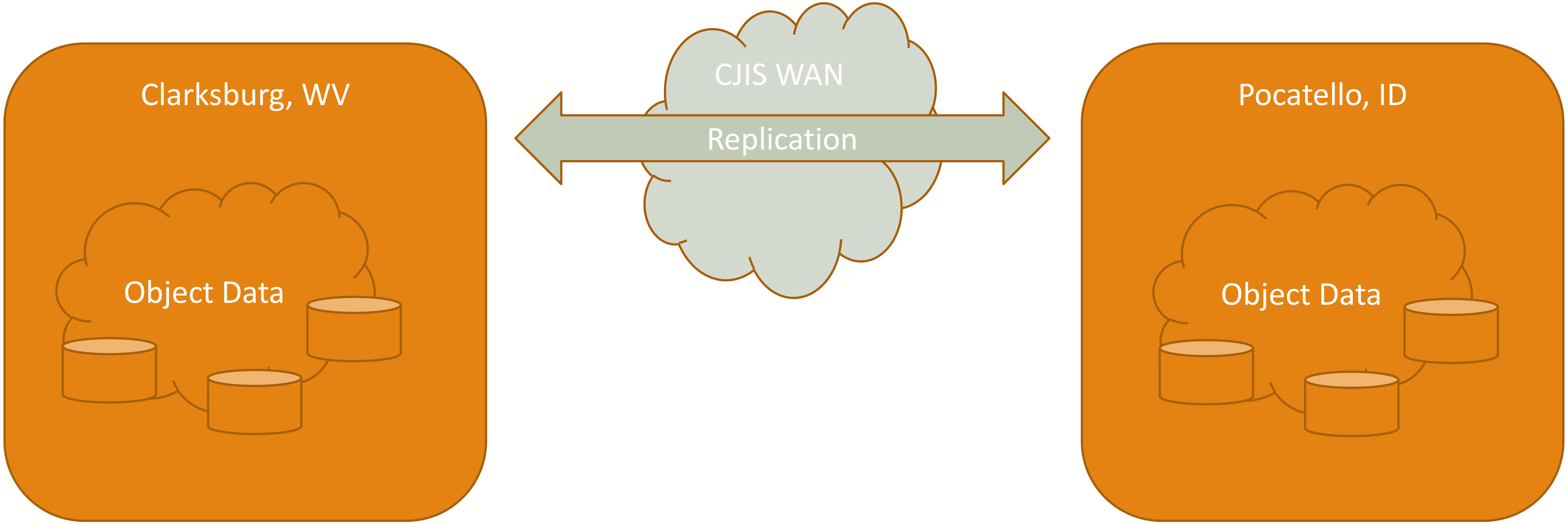
Pre 2012 – Data only @ CJIS



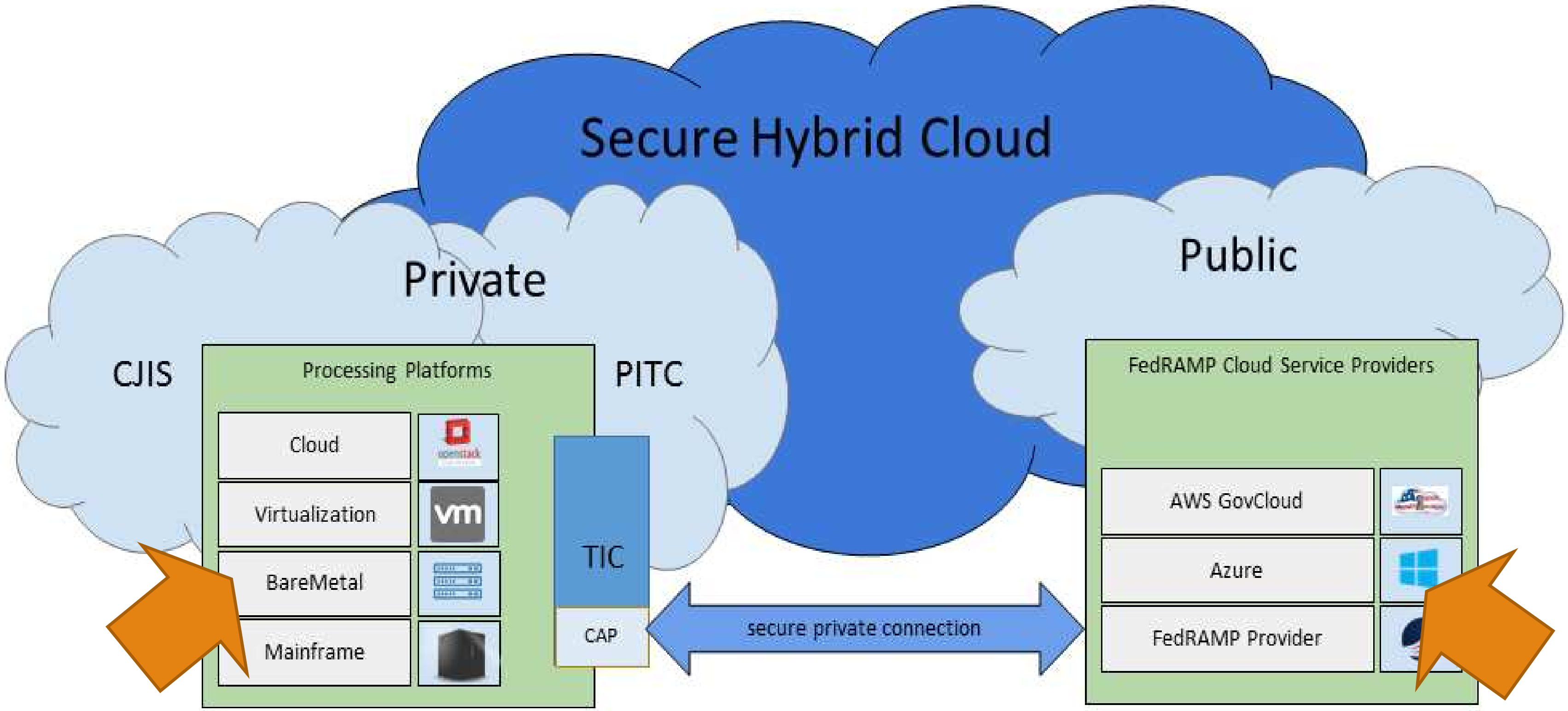
CJIS business need to run object storage services in multiple data centers in order to maximize availability.

- Recognize that we will have to deal with unlike HW / storage technologies in each data center.

2013 – Established DR @ PITC



2016 Concept



On-Premises Cloud Services; Virtual and Physical Servers; and Mainframe Infrastructure

Off-Premises Cloud IaaS

Initial Security Constraints for Off-Prem Cloud Services

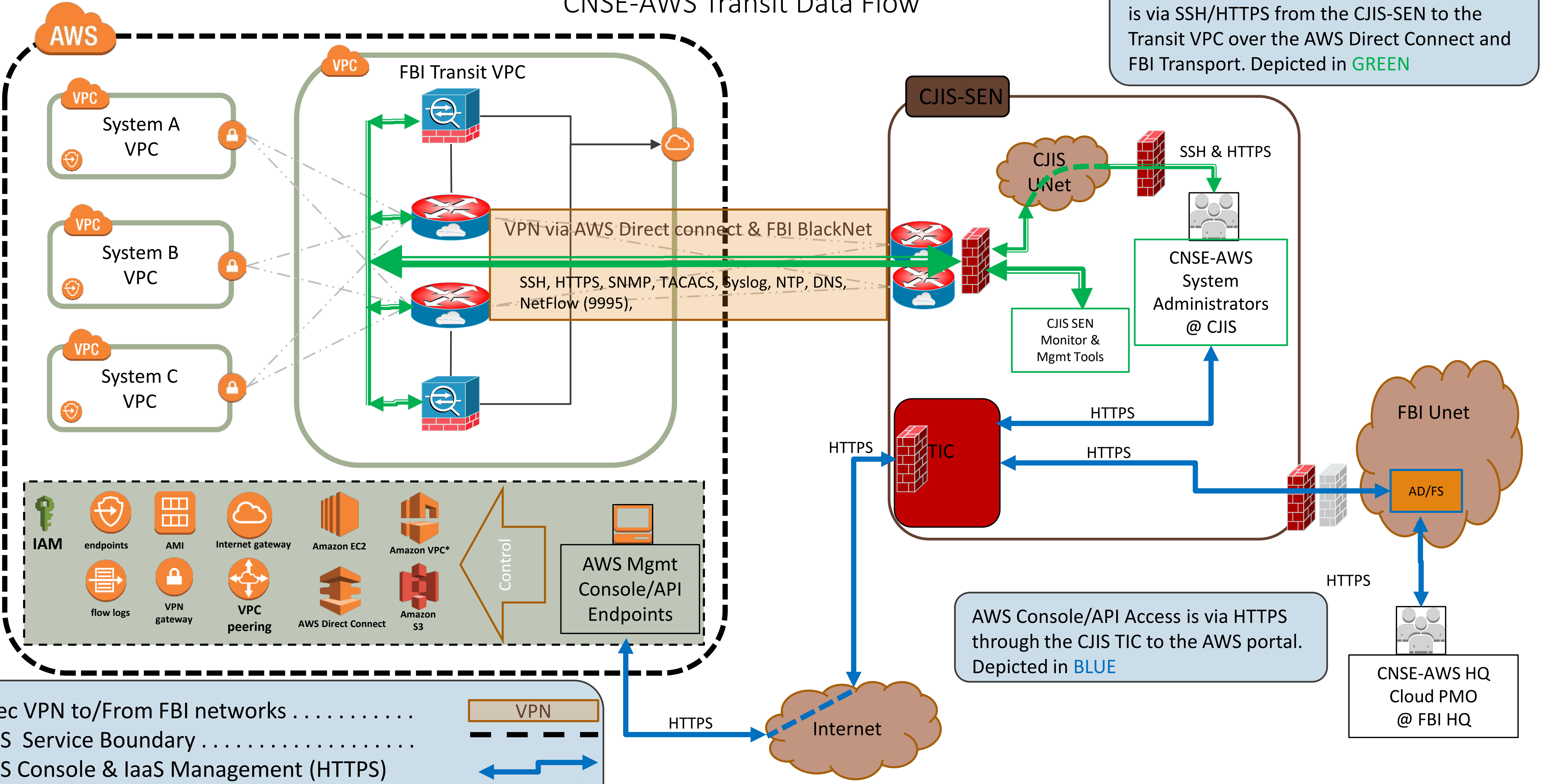
- ❑Must only use FedRAMP High IaaS Gov Cloud
- ❑Services must also be FedRAMP High
- ❑All data encrypted at rest
- ❑All data encrypted in transit
- ❑All encryption keys managed by FBI
- ❑All authentication 2-Factor

AWS Chosen to meet Business Need

- ❑FBI Deputy CIO came from CIA and was part of CIA's TS AWS
- ❑ Existing C2S Contract with AWS available for use
- ❑ Trending Idea that RedHat=AWS and Windows=Azure
- ❑ CJIS Developers had more AWS experience than Azure experience

CNSE-AWS Transit Data Flow

AWS Transit component management access is via SSH/HTTPS from the CJIS-SEN to the Transit VPC over the AWS Direct Connect and FBI Transport. Depicted in GREEN



AWS Console/API Access is via HTTPS through the CJIS TIC to the AWS portal. Depicted in BLUE

IPSec VPN to/From FBI networks . . . . VPN

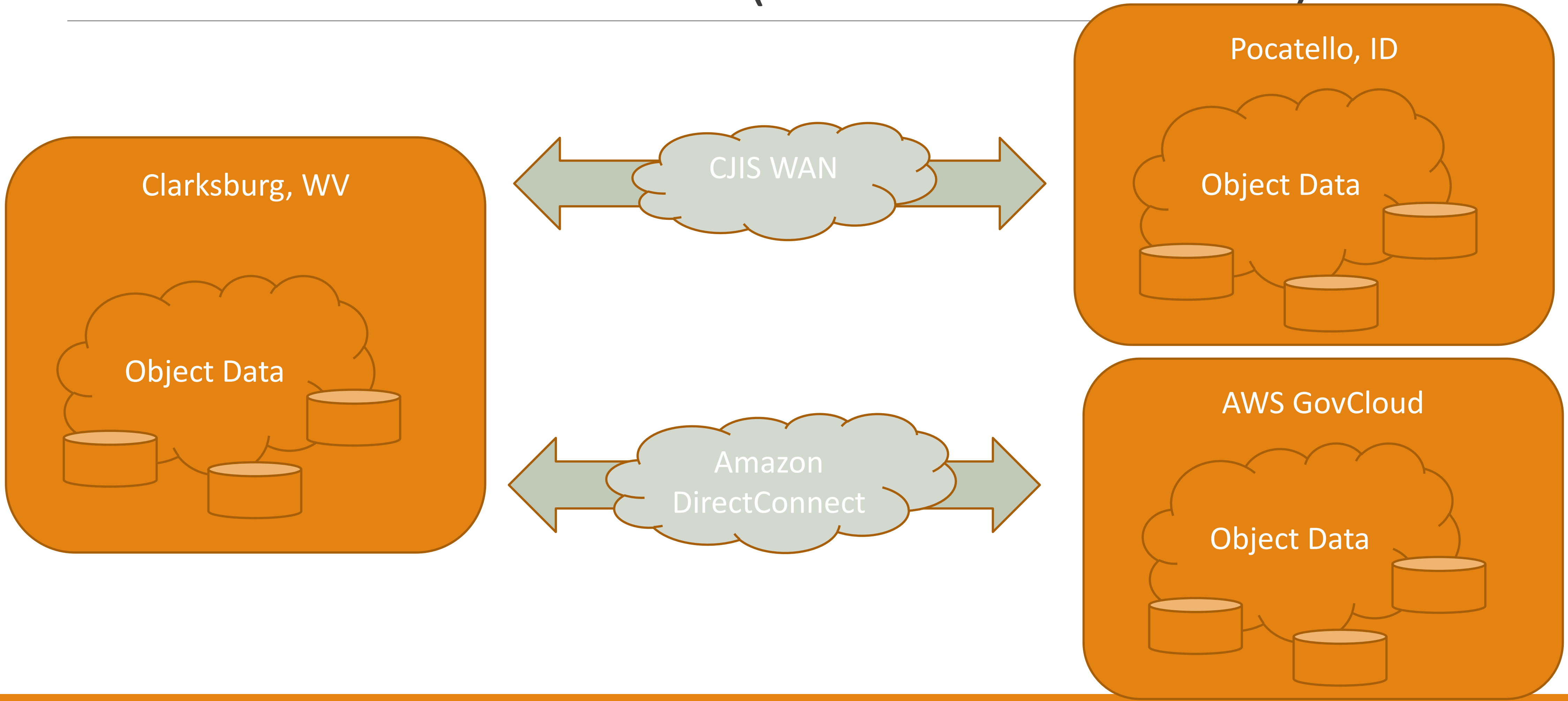
AWS Service Boundary . . . . ▬ ▬ ▬

AWS Console & IaaS Management (HTTPS) ⟷

CNSE Component Management (SSH & HTTPS) ⟷

Routed FBI Traffic via IPSec VPN Connections - · - · -

2017 – Add 3rd site (AWS GovCloud)



Replication Timeline

Replication from CJIS to AWS GovCloud

-- The OE replication started on 8/16/2017 after much testing and security approvals.

-- The bulk replication completed sometime near the end of January 2018.

-- Verification from Feb 1, 2018 – May 4, 2018.

-- Amount: approximately 17 billion objects replicated

-- Environments: OE and NOE

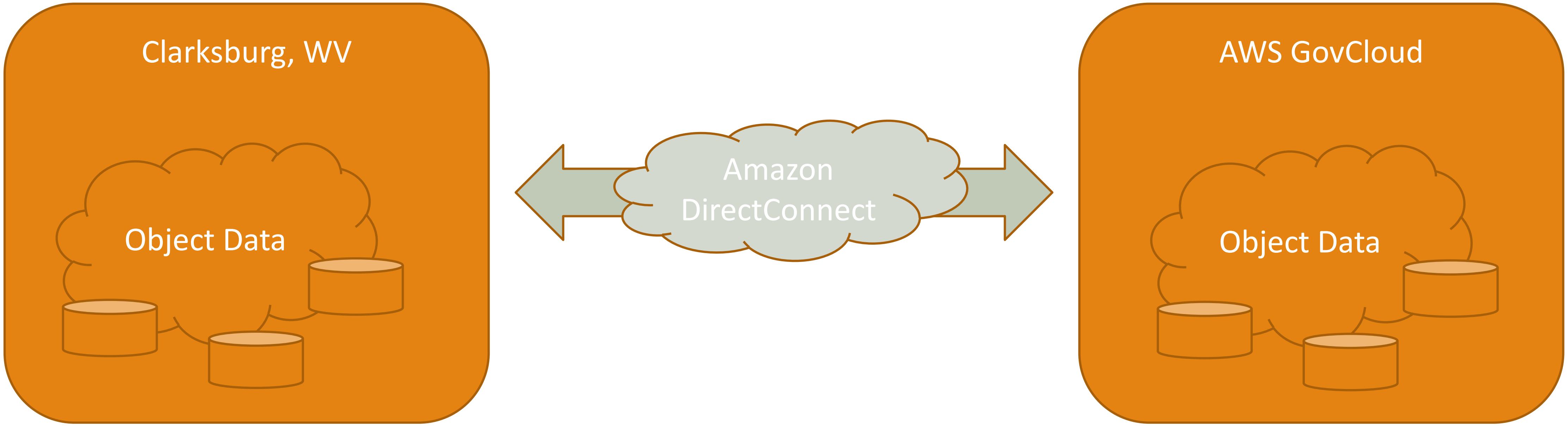
Performance Testing AWS vs. PITC

Size of Obj	AWS	PITC
Small (200 bytes)	402 ms	253 ms
Medium (14 KB)	410 ms	379 ms
Large (3-12 MB)	2,421 ms	15,557 ms

Security Testing and Approvals

- ❑Validation of FedRAMP package
- ❑Mapped package to NIST Controls to determine inheritance
- ❑Identified non-inherited controls were implemented for compliance
- ❑Validated restrictions on IGWs
- ❑Validated roles within AWS account structure
- ❑Automated testing of images and path infrastructure (working with AWS on future auto testing)
- ❑Manual assessments object store
- ❑Validated encryption
- ❑Approval to test
- ❑Approval to Operate

2018 – remove Pocatello



Some Lessons Learned

- ❑ It takes a village to raise a hybrid cloud
- ❑ Not all FedRAMP services are ready for the gov cloud
- ❑ Choose the right encryption service
- ❑ Must enforce 2FA on management console
- ❑ Cloud IAM is challenging if on-prem isn’t already enterprise IAM
- ❑ Establishing account roles and keeping them current is a political minefield
- ❑ Model your data flows and understand capacities before choosing your cloud service provider
- ❑ Implementers must be learners and teachers
- ❑ Pace of change keeps difficulty at a high level

Questions?