

A large, semi-transparent watermark of the FBI seal is centered behind the text. The seal features a circular design with "DEPARTMENT OF JUSTICE" at the top, "FEDERAL BUREAU OF INVESTIGATION" around the bottom, and "FIDELITATEM PRO TERRAM" on the left. In the center is a shield with scales and a sword.

ISO Symposium

August 16, 2017

FBI CJIS Information Security Officer Staff

A collage of international welcome words surrounding the word "Welcome" in large black letters. The words include: Namaste (Hindi), Toivottaa (Finnish), Heten. (Swedish), Begr. (Norwegian), Mirepres (Spanish), iBiala (Polish), Dobrodošli (Croatian), Selamat Datang (Indonesian), Hospedar (Portuguese), nης (Greek), éni (Hungarian), Bonvenon (French), Sambut (Indonesian), Bienvenido (Spanish), and Acollier (French). The background is a blurred image of a beach.

Agenda

Morning:

- 8:45 – APB Overview
- 9:15 – Compact Overview
- 9:45 – Break
- 10:15 – Audit
- 11:15 – SA Subcommittee Panel

Afternoon:

- 1:30 – Policy Updates & Topics on the Horizon
- 2:15 – Top Policy Concerns Use Case Panel, Part 1
- 3:15 – Break
- 3:45 – Top Policy Concerns Use Case Panel, Part 2
- 4:45 – Closing Remarks
- 7:00 – P2P Discussions



FBI/CJIS Advisory Policy Board



CJIS Services



Shared management – APB

the FBI along with federal, local, state and tribal data providers and system users share responsibility for the operation and management of all systems administered by the CJIS Division for the benefit of the criminal justice community.

Subs

CJIS Advisory Process – Working Groups

to obtain the user community's advice and guidance on the operation of all of the CJIS programs.

CJIS Services



Advisory Policy Board (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



Advisory Policy Board (APB)

*What does the APB
do?*



The APB made approximately 60 recommendations over the past year (December 2015/June 2016). Some of the more notable recommendations include:

10 Key Recommendations

- Transition the nation to NIBRS only reporting (sunset UCR Summary) by January 2021
- Collection and reporting of police officer Use of Force statistics
- 14 foundational concepts for the next generation of NCIC (N3G)
- Policies on the use of the Interstate Photo System
- Policies to allow Fusion Centers access to criminal history records through cooperative agreements with criminal justice agencies
- Creation and publication of a Disposition Best Practice Guide
- Criminal Justice RapBack Guide updates
- Updates to Mobile Device Security
- Rapid DNA submission requirements



A few upcoming topics for the December 2017 APB Meeting

- Embargo Data Policies within UCR
- N3G concept requirements (Concepts 2, 4, 8, 13)
- Expansion of UCR Police Employee Collection
- Required information in NICS Indices submission
- CJIS Security Policy Restrictions for Criminal Justice Information stored in offshore cloud facilities



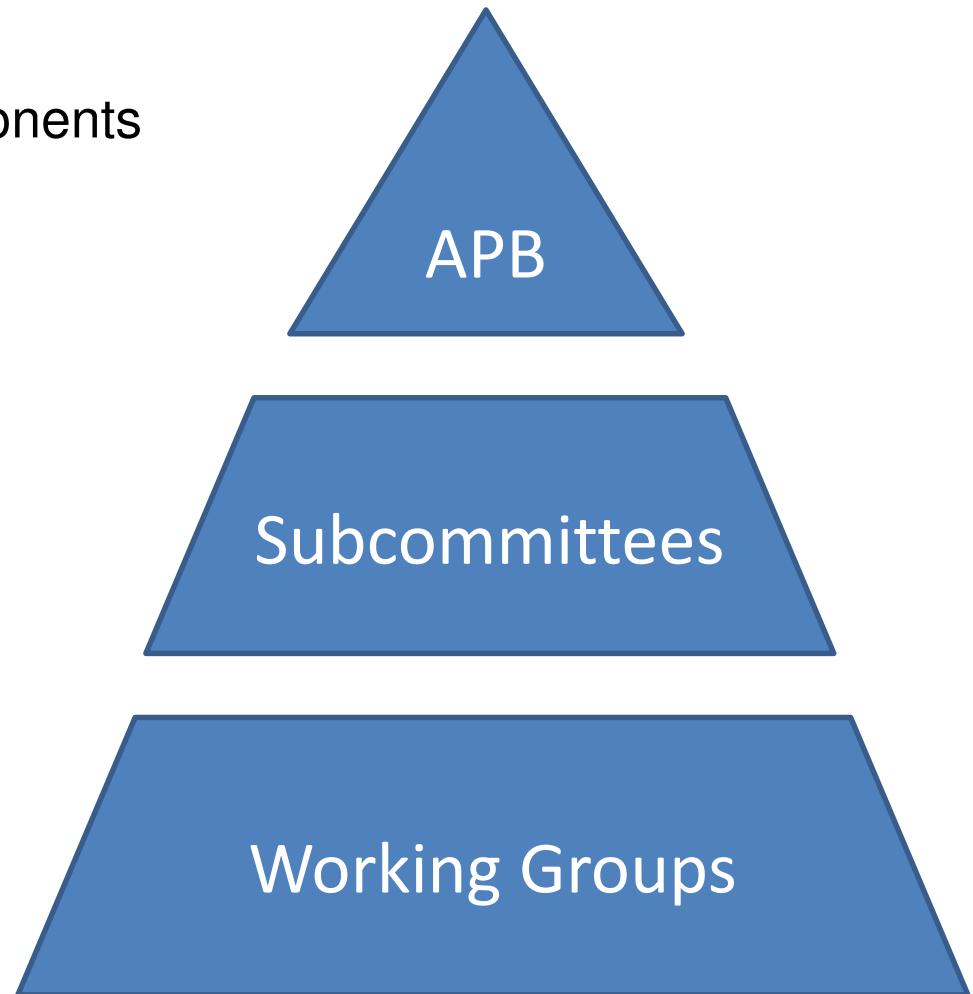
Advisory Policy Board (APB)

*How does the APB
process work?*



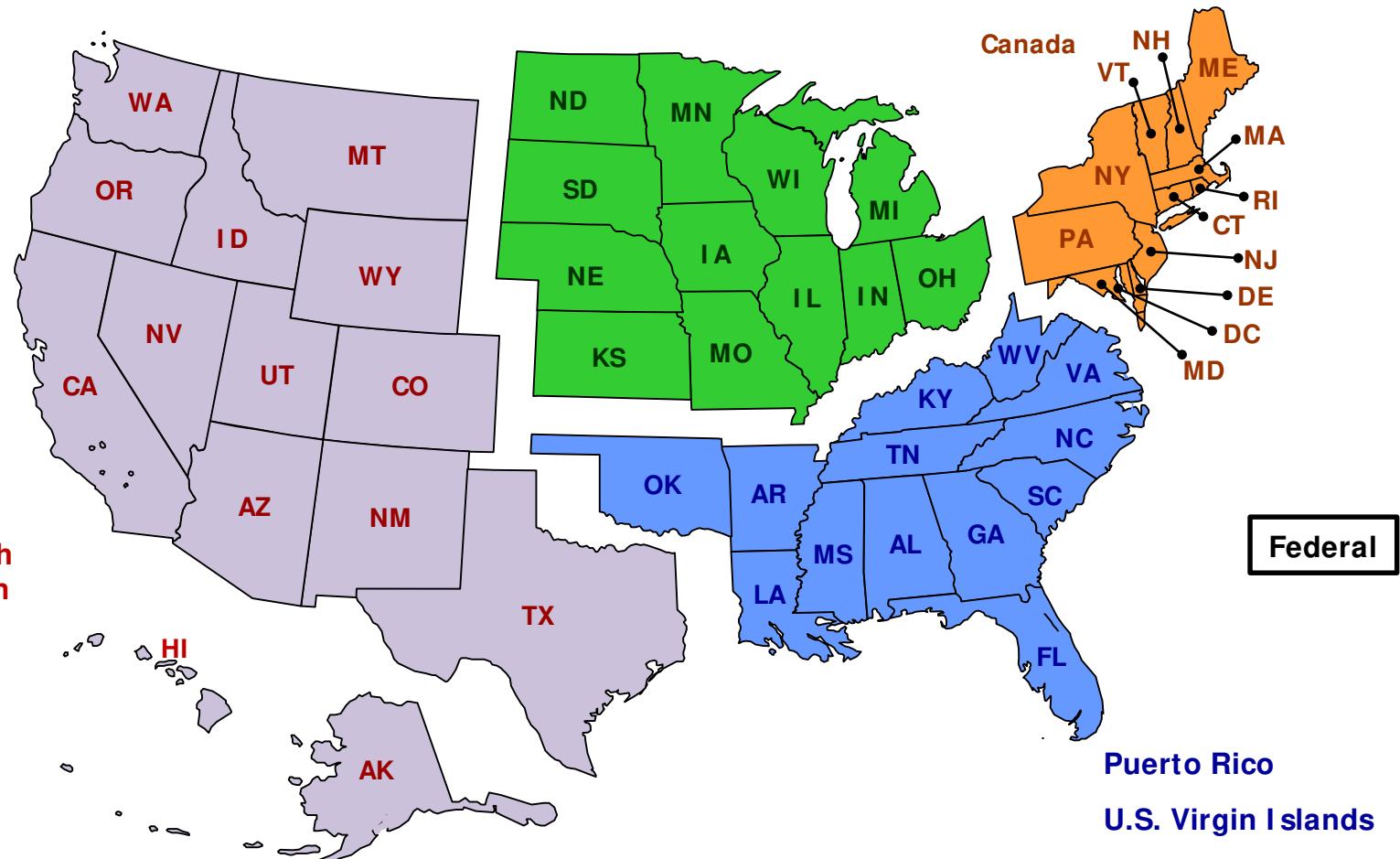
Advisory Policy Board (APB)

The Process has 3 main components



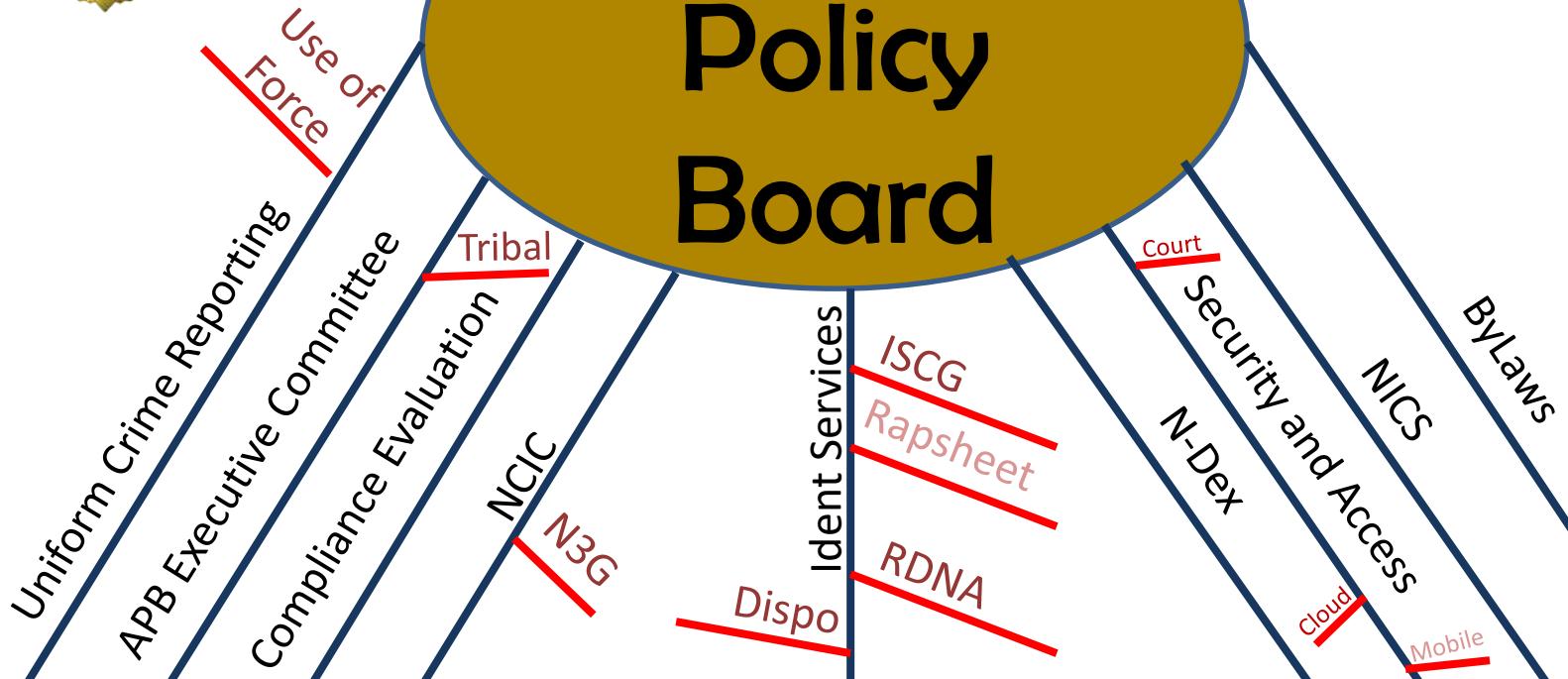


Advisory Policy Board Working Group Regions

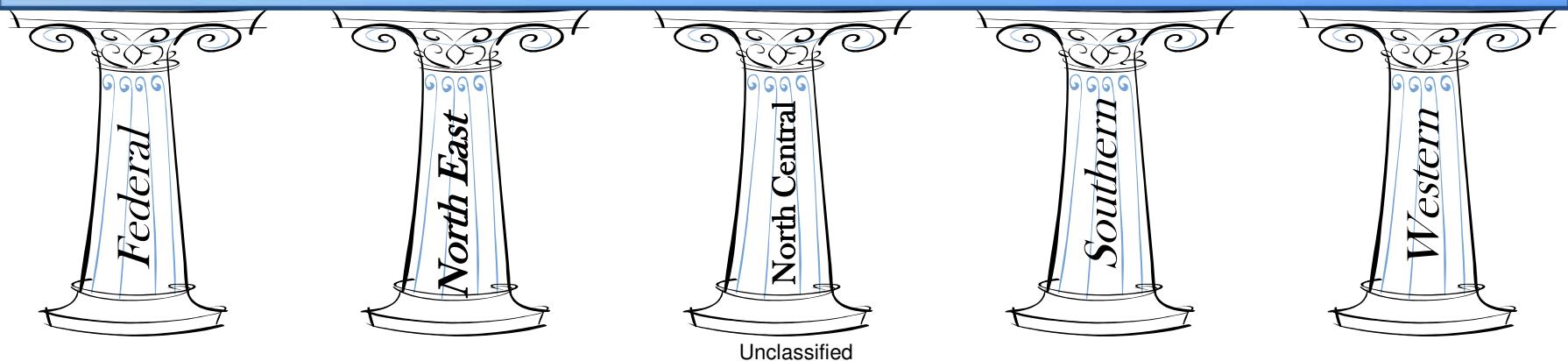




Advisory Policy Board



Working Groups





Recommendations to the Director of the FBI

**Advisory
Policy
Board**

Implementation



Advisory Policy Board (APB)

Who is on the APB?



APB Representation

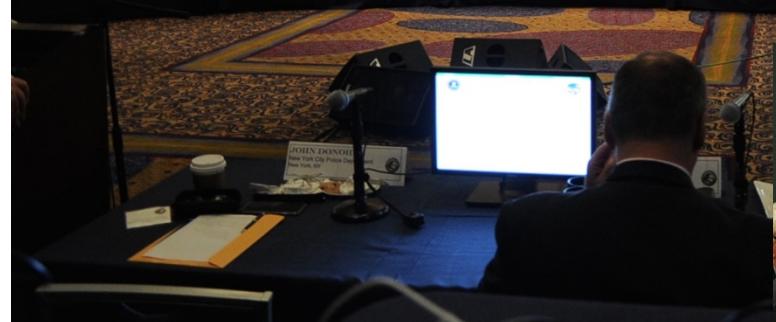
The following representatives make up the APB

- 35 members
 - 20 selected by the four regional Working Groups
 - 12 state agency representatives
 - 8 local agency representatives
 - 1 Selected by the Federal Working Group
 - 5 FBI Director appointees
 - 1 represents judiciary agencies
 - 1 represents prosecutorial agencies
 - 1 represents correctional agencies
 - 1 individual representing national security
 - 1 tribal law enforcement representative



APB Representation

- 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 Compact Council representative from a Criminal Justice Agency





Unclassified



APB Quick Facts

- 2000
 - The approximate number of APB recommendations approved by the Director since 1994.
- >200
 - Number of individuals involved in the process
- 25
 - Approximate number of APB WGs, Subs, Task Forces, and Boards
- 58
 - Number of APB recommendations in Fiscal Year 16



Advisory Process Board



- APB Chair
- Assistant Chief John Donohue
Commanding Officer
New York City Police Department



- APB 1st Vice Chair
- Assistant Director Mike Lesko
Law Enforcement Support Division
- Texas Department of Public Safety



Advisory Process Board



- APB 2nd Vice Chair
- Deputy County Manager for Public Safety
- Henrico County Manager's Office



- Designated Federal Officer
- R. Scott Trent
FBI/CJIS Division
304-625-5263



Questions or comments?

Please contact:

R. Scott Trent

Designated Federal Officer

304-625-5263

rstrent@fbi.gov

The National Crime Prevention and Privacy Compact/Compact Council



The National Crime Prevention And Privacy Compact Act



Implemented on October 9, 1998
42 U.S.C. 14611-14616

Provides federal authority for the interstate exchange
of state criminal history record information (CHRI)
for noncriminal justice purposes

Importance of the Compact

- Assured Record Availability
- Uniform Interstate Dissemination
 - Emphasizes state-centric exchange
- Balances privacy with availability of records
- Mechanism to promulgate rules and establish procedures

Responsibilities of the State Compact Officer

- Administer the Compact within the State;
- Ensure that Compact provisions and rules, procedures, and standards established by the Council are complied with in the state; and
- Regulate the in-State use of records received by means of the III System from the FBI or from other Party States

Establishment of Compact Council and Authority

Article VI – Establishment of Compact Council

- Which shall have the authority to promulgate rules and procedures governing the use of the III System for noncriminal justice purposes.

The Council may only promulgate rules and procedures for access to CHRI for noncriminal justice purposes, based on existing statutory authority.

Compact Council

15 Members Appointed by the US Attorney General

9 – State Compact Officers

2 – At large members nominated by the FBI Director

2 – At large members nominated by the Council Chair

1 – FBI/CJIS Advisory Policy Board member

1 – FBI employee nominated by the FBI Director

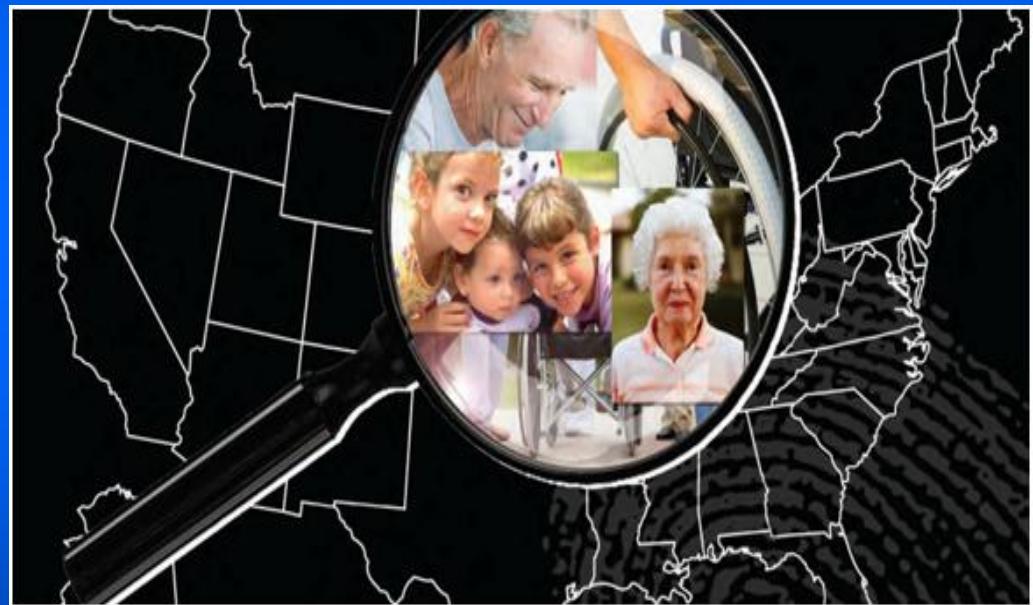
How does the Council Conduct Business?



Crime Prevention

Protecting Vulnerable Populations such as Children, the Disabled, and the Elderly

- Publication of Identity Verification Program Guide
- Use of CHRI in exigent circumstances
- National Noncriminal Justice Rap Back Service



Privacy Protections

- Guiding Principles for Privacy Protection
- Fingerprint requirement for accessing CHRI
- National Fingerprint File



28 CFR 906

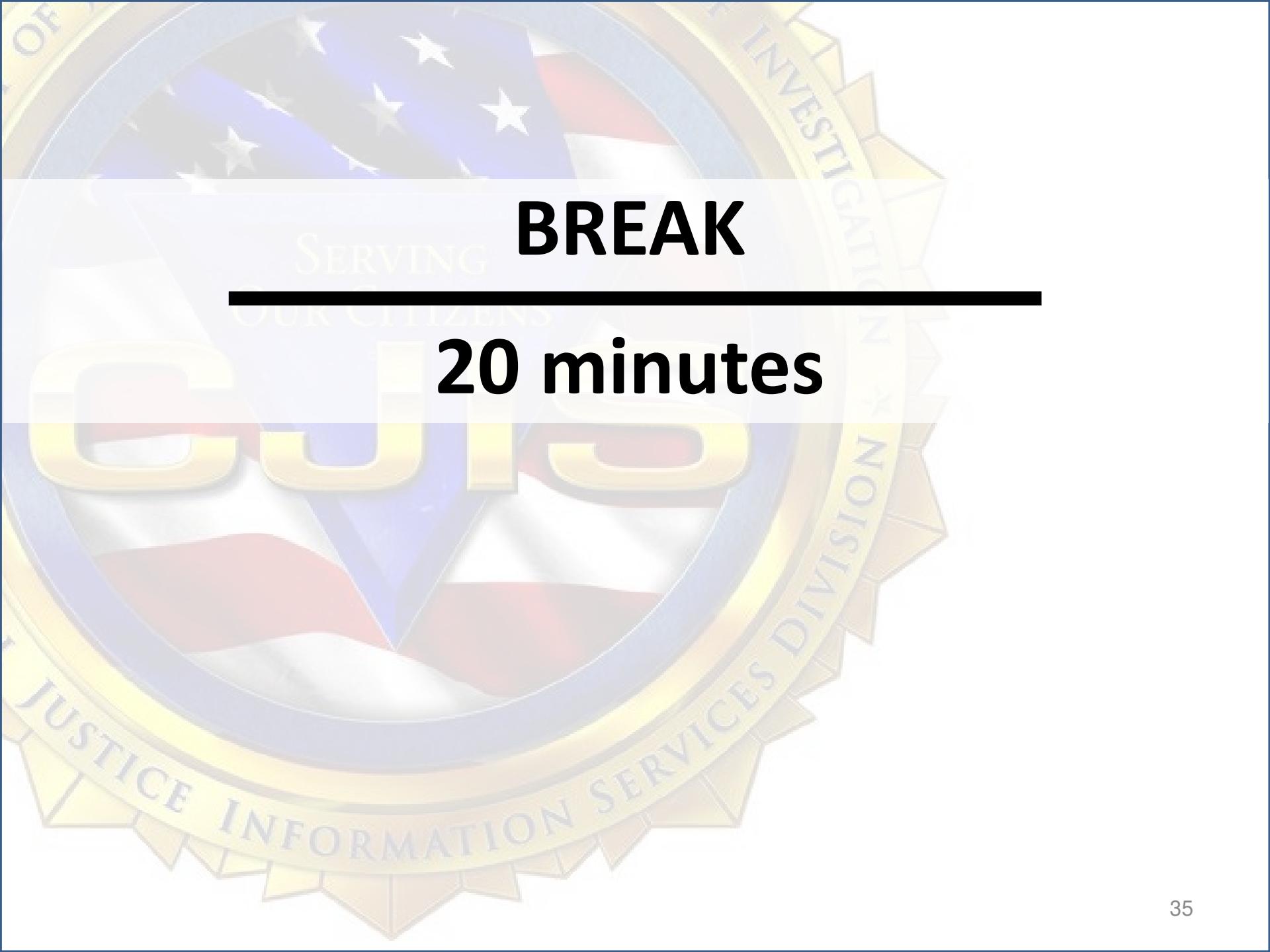
Outsourcing of Noncriminal Justice Administrative Functions

- Establish rules and procedures for third parties to perform noncriminal justice functions involving access to III
- Security & Management Control Outsourcing Standard
 - Channelers
 - Non-Channelers
- Outsourcing Guides

FBI Compact Officer

Chasity S. Anderson
304-625-2803
csanderson@fbi.gov

<https://www.fbi.gov/services/cjis/compact-council>

A faint watermark of the Federal Bureau of Investigation seal is visible in the background. The seal features a shield with stars and stripes, surrounded by a circular border with the words "DEPARTMENT OF JUSTICE", "FEDERAL BUREAU OF INVESTIGATION", and "Serving Our Citizens".

BREAK

20 minutes

CJIS IT Security Audit

**Derek Holbert / Candice Preston
FBI CJIS IT Security Auditors**

Security & Access Subcommittee

Task Force Panel

Moderator: Chris Weatherly

FBI CJIS Information Security Officer Program Manager

SA TASK FORCE PANEL

Panelists:

- Brad Truitt – SA Subcommittee Chair
- Patrick Woods – Cloud Task Force Chair
- Brenda Abaya – Mobile Task Force Chair
- Corey Steel – Courts Task Force Chair
- George White – FBI CJIS ISO

A faint watermark of the Federal Bureau of Investigation seal is visible in the background. The seal features a shield with stars and stripes, surrounded by a circular border with the words "DEPARTMENT OF JUSTICE" and "FEDERAL BUREAU OF INVESTIGATION".

LUNCH

12:00 – 1:30p

CJIS Security Policy

v5.6 Changes

Jeff Campbell

FBI CJIS Assistant Information Security Officer

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).

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

“On the Horizon”

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

Note: Approved means APB approved.

CJIS SECURITY POLICY OVERVIEW

Fall 2017 APB Topics

SERVING
OUR CITIZENS

	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			Time Stamps	The agency's information system shall provide time stamps for use in audit record generation.	2	Both	Both	Service Provider
219	5.4.4	5.4.4	"	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			Audit Record Retention	The agency shall retain audit records for at least one (1) year.	1	Both	Both	Service Provider
223	5.4.6	5.4.6	"	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			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	5.4.7	5.4.7	"	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

CJIS SECURITY POLICY OVERVIEW

Fall 2017 APB Topics

- **Restriction of off-shore storage of data**
- **Section 5.12 changes**
- **Vetting of non-U.S. citizens**

FBI CJIS ISO Resources

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@ic.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 for each requirement
- Includes the “Cloud Matrix”
- Updated annually in conjunction with the CJIS Security Policy

iso@ic.fbi.gov

ISO RESOURCES

CJIS Security Policy Mapping to NIST 800-63 rev 4

- Companion 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@ic.fbi.gov

ISO RESOURCES

CJIS Security Policy Resource Center

- Publicly available

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

- Features
 - Search and download the current Policy version
 - Requirements Companion Document
 - Cloud Report & Control Catalog
 - Use Cases, Mobile Appendix, Links of Importance, NIST Mapping
 - Submit a Question (to entire ISO staff)

iso@ic.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](#)
[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](#) | [2016 ISO Symposium Presentations](#) | [Use Cases](#) | [Cloud Computing Report](#) | [Cloud Report Control Catalog](#) |
[Mobile Appendix](#) | [Submit a Question](#) | [Links of Importance](#)

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

DOCUMENT PAGES Zoom

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

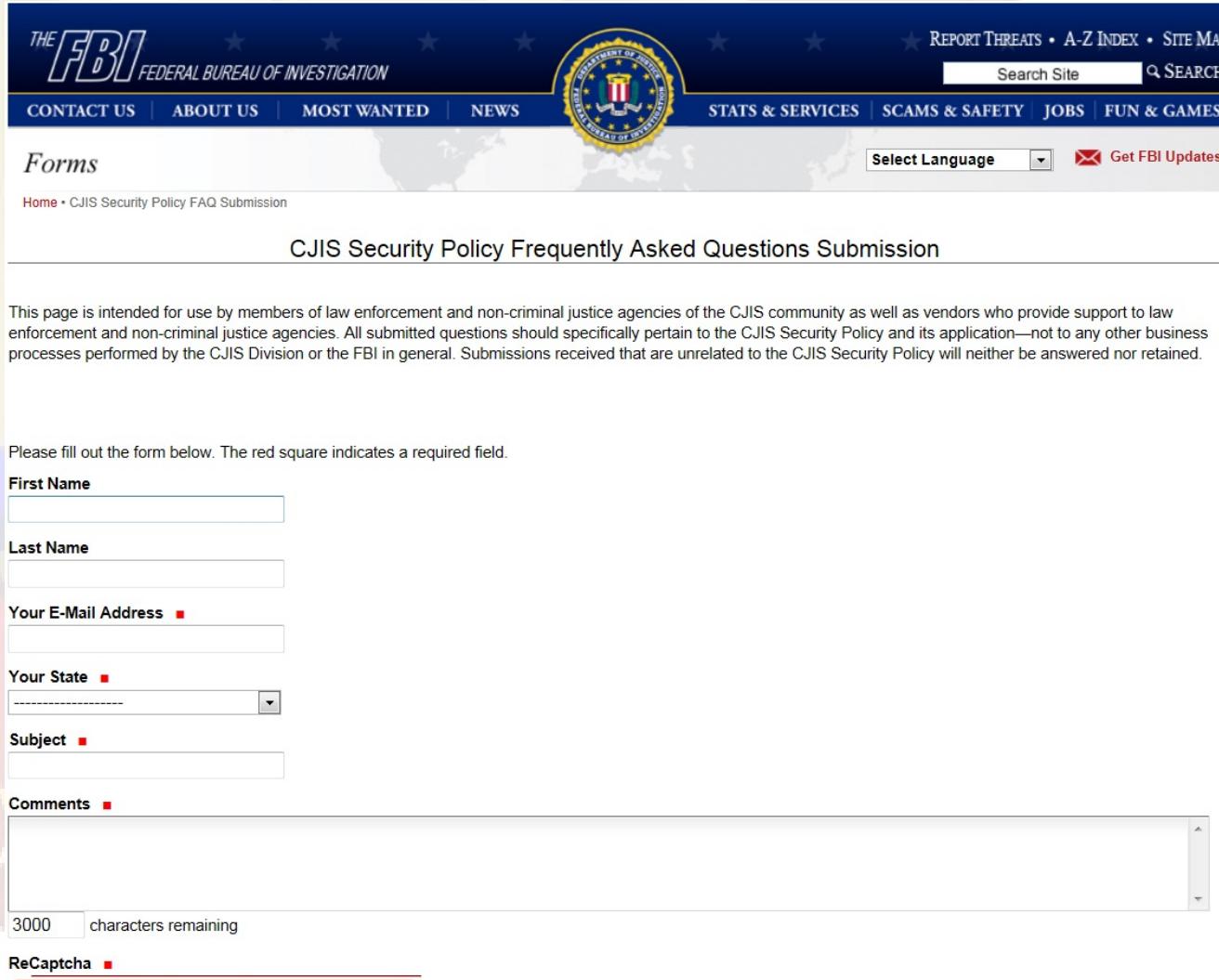
FAQs

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>



The screenshot shows the official website of the FBI's CJIS Security Policy Resource Center. The header features the FBI logo and navigation links for REPORT THREATS, A-Z INDEX, and SITE MAP. Below the header is a search bar with a "SEARCH" button. The main menu includes CONTACT US, ABOUT US, MOST WANTED, NEWS, STATS & SERVICES, SCAMS & SAFETY, JOBS, and FUN & GAMES. A "Forms" section is highlighted. On the right, there are options to "Select Language" and "Get FBI Updates". The page title is "CJIS Security Policy Frequently Asked Questions Submission". A descriptive text explains the purpose of the form, stating it is for members of law enforcement and non-criminal justice agencies regarding the CJIS Security Policy. The form itself consists of several input fields: First Name, Last Name, Your E-Mail Address, Your State (a dropdown menu), Subject, Comments (a large text area), and a character count indicator (3000 characters remaining). A ReCaptcha field is at the bottom.

THE **FBI** FEDERAL BUREAU OF INVESTIGATION

REPORT THREATS • A-Z INDEX • SITE MAP

Search Site

CONTACT US | ABOUT US | MOST WANTED | NEWS |  STATS & SERVICES | SCAMS & SAFETY | JOBS | FUN & GAMES

Forms

Home • CJIS Security Policy FAQ Submission

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 Office LEEP SIG

SPECIAL INTEREST GROUPS
SECURING THE NATION THROUGH RESPONSIBLE INFORMATION SHARING

FEDERAL BUREAU OF INVESTIGATION

Highlights **RSS News Feed** ▾ **SIGs** **Special Topics** **Forums** **Resources**

IN

Services
Email
Member Services

Partnered Sites
NCIRC.gov
eGuardian
ORION
NCMEC
NamUs
NGIC
VICAP

Professional Opportunities

Accessibility Statement
Administrative Note
SIG/VCC Brochure
Privacy Policy
User Survey

CJIS-ISO Home **SIG Services** ▾

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.

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

+ Add to MySIGs

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 Manager & 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

My VCCs
VCC
Open VCCs
VCC-1
Unopened VCCs
VCC-7

My SIGs
Member Link **Public**
CJIS CJIS - I
CJIS-ISO CJIS T
CJISTRIBAL Cyber S
CSA Nations
NCIC Nations
NCPCC Nations
Council

Quick Links
Law Enforcement
National Alert Syst
Internet Crime Co
Officers Killed and
Create a SIG
Request a VCC
Law Enforcement

Spotlights

Active Shooter Res

CJIS ISO CONTACT INFORMATION

George White
FBI CJIS ISO

(304) 625 - 5849

george.white@ic.fbi.gov

Chris Weatherly
FBI CJIS ISO Program Manager

(304) 625 - 3660

john.weatherly@ic.fbi.gov

Jeff Campbell
FBI CJIS Assistant ISO

(304) 625 - 4961

jeffrey.campbell@ic.fbi.gov

Steve Exley
Sr. Consultant/Technical Analyst

(304) 625 - 2670

stephen.exley@ic.fbi.gov

iso@ic.fbi.gov

“Top Policy Concerns”

Use Case Scenarios Panel

Moderator: Chris Weatherly

FBI CJIS Information Security Officer Program Manager

USE CASE SCENARIO PANEL

Panelists:

- **Ronnie George – CJIS IT Security Auditor**
- **Candice Preston – CJIS IT Security Auditor**
- **Steve Exley – CJIS ISO Program**
- **Jeff Campbell – CJIS ISO Program**

USE CASE SCENARIO PANEL

Category: Encryption

Scenario #1: Backup drives containing CJI in storage

Scenario:

A 911 Dispatch Center creates backup tapes of their RMS system, which contain CJI, and stores the tapes at a rented warehouse where all other city departments stored their backups. All city departments have access to the facility, but not all personnel have been fingerprinted or completed security awareness training in accordance with the *CJIS Security Policy*.

Question: Is encryption required for the CJI while at rest in this location?

USE CASE SCENARIO PANEL

Category: Encryption

Facts:

- CJI stored on backup drives
- CJI backup drives stored in warehouse facility
- Warehouse storage area does not restrict access to authorized personnel

Answer: Yes

This area is not a physically secure location. Therefore, encryption for data at rest is required in accordance with *CJIS Security Policy* Section 5.10.1.2.2. – use a module that is FIPS 140-2 certified and use a symmetric cipher key strength of at least 128 bit in strength, OR use a solution that provide a symmetric cipher that is FIPS 197 certified (AES) and at least 256 bit in strength.

USE CASE SCENARIO PANEL

Category: Encryption

Scenario #2: CJI Stored in a local RMS

Scenario:

The CSA maintains a disaster recovery (DR) site that is managed by a state consolidated IT Department in a different part of the city. Backups of all information systems, including those containing CJI, are replicated and stored in to a virtual storage area network (SAN) at the remote DR site. The CSA is not required to encrypt the CJI while at rest at the CSA, because it is in a physically secure location. The DR site is also a physically secure location.

Question: Is encryption required for the CJI in transit between the CSA and DR site?

USE CASE SCENARIO PANEL

Category: Encryption

Facts:

- CJI is not encrypted at rest
- CJI is replicated at the CSA
- CJI is replicated and stored at rest in a physically secure location
- CSA and DR site are different locations

Answer: Yes

CJI is transmitted outside the boundary of the physically secure location to the DR site, so encryption is required to protect CJI while in transit to the DR site in accordance with *CJIS Security Policy* Section 5.10.1.2.1. – use a module that is FIPS 140-2 certified and use a symmetric cipher key strength of at least 128 bit in strength.

USE CASE SCENARIO PANEL

Category: Management Control Agreement (MCA)

Scenario #3: Outsourced IT Administration

Scenario:

A County Sheriff's Office (SO) is receiving IT services from the County Department of Information Technology (DoIT). IT services include desktop support and network administration. The information systems serviced by the DoIT contain CJI and are housed at the county IT data center, which is a physically secure location, with all other county government departments. All County IT personnel are authorized personnel and have unescorted access to the data center. The CJI is not encrypted at rest.

Question: Is an MCA required between the Sheriff's Office and the DoIT?

USE CASE SCENARIO PANEL

Category: MCA

Facts:

- County SO is a CJA
- DoIT is a NCJA
- A CJA has outsourced IT service to a NCJA
- NCJA personnel have unescorted access to unencrypted CJI
- NCJA personnel perform IT services on CJI-processing systems – admin right

Answer: Yes

An MCA is required between the County SO (CJA) and the DoIT (NCJA). The MCA is designed to ensure the CJA maintains management control over the protection of the CJI in the NCJA's environment and to ensure *CJIS Security Policy* compliance.

USE CASE SCENARIO PANEL

Category: Management Control Agreement (MCA)

Scenario #4: Outsourced Custodial Services

Scenario:

The City Police Department (PD) is receiving custodial services from the City Facilities Department. The custodial personnel have completed security awareness training (level 1) and have passed the proper fingerprint-based background checks. All custodial personnel are allowed unescorted access to the PD, including the secure terminal areas (physically secure locations).

Question: Is an MCA required between the City PD and the City Facilities Department?

USE CASE SCENARIO PANEL

Category: MCA

Facts:

- City PD is a CJA
- City Facilities Department is a NCJA
- A CJA has outsourced custodial services to an NCJA
- NCJA personnel have unescorted access to physically secure locations – authorized personnel
- NCJA personnel are not performing criminal justice functions

Answer: No

An MCA is not required in this scenario. Although the custodial personnel are noncriminal justice governmental employees and have unescorted physical access to the secure areas with CJI, cleaning and maintenance services are not considered criminal justice functions.

USE CASE SCENARIO PANEL

Category: Security Addendum (SA)

Scenario #5: Contracted Cloud Storage of RMS

Scenario:

The County SO is using a local cloud storage company to store backups of their RMS systems as part of the DR coop plan. The RMS backups include CJI. The backups are encrypted by the County SO IT prior to being sent to the cloud company via Internet connection. The SO manages the crypto key infrastructure. The cloud vendor cannot decrypt the data.

Question: Is an SA required to be signed by the cloud service provider?

USE CASE SCENARIO PANEL

Category: SA

Facts:

- County SO is a CJA
- Cloud service provider is a private contractor
- Cloud provider is performing a criminal justice function – media storage

Answer: No

- CJI encrypted CJI prior to transmission to the cloud
- CJA maintains the crypto keys; cloud provider does not have access to the keys
- Cloud provider only has access to encrypted CJI – “ball of mud”

The SA is not required in this scenario. While, the cloud service provider personnel are private contractors and are performing the ‘criminal justice function’ of media storage, no contractor personnel of the cloud storage facility have unescorted access to unencrypted CJI. The CJI is encrypted by the CJA who is also managing the keys, and therefore it cannot be unencrypted or accessed by outside personnel.

USE CASE SCENARIO PANEL

Category: Security Addendum (SA)

Scenario #6: Subcontracted media destruction

Scenario:

A local PD has outsourced IT services and media destruction services to the City IT Dept. City IT personnel are authorized personnel and have unescorted access to unencrypted CJI. The City IT Dept. has a subcontract with a local company for physical and electronic media destruction of all the city's media, which includes the PD's. The PD's media contains unencrypted CJI. Local contractor company personnel have unescorted access to unencrypted CJI for destruction purposes. They have been vetted and security awareness trained, but have not signed the SA.

Question: Is an SA required to be signed by the local contractor personnel?

USE CASE SCENARIO PANEL

Category: SA

Facts:

- City PD is a CJA
- City IT Dept. is a NCJA (Gov.)
- MCA in place: CJA <-> NCJA
- Local media destruction company is a private contractor
- Both NCJA and contractor perform criminal justice functions
- Contractor has background checks and security awareness training

Answer: Yes

The SA is required for each individual contractor with unescorted access. The contractor personnel are performing the criminal justice function of media destruction and have unescorted access to unencrypted CJI.

USE CASE SCENARIO PANEL

Category: Advanced Authentication (AA)

Scenario #7: Access to query CJI from an RMS

Scenario:

A City PD is using RMS software from a private contractor. Private contractor personnel remote login at their leisure/discretion (session is not initiated by the PD) to this RMS server to perform administrative support. The RMS has connectivity to the state switch and can initiate transactions directly to the state. The RMS is located within a physically secure location, the contractor location may not be. To access the RMS, the contractors use an encrypted VPN and authenticate to the network via a username and password.

Question: Is AA required in this scenario?

USE CASE SCENARIO PANEL

Category: AA

Facts:

- Remote access to CJI
- Remote access from uncontrolled/unknown locations
- System has direct access to CJI
- Username provides identification
- Password provides authentication (something you know)

Answer: Yes

The private contractor personnel have remote access (access outside the physically secure location) to a direct access information system. The current solution will need to be modified to include AA.

USE CASE SCENARIO PANEL

Category: Advanced Authentication (AA)

Scenario #8: Access to CJI Stored in a local RMS

Scenario:

A County SO has created a local RMS. The RMS does not have connectivity to any state or federal CJIS systems, but contains CJI. The RMS is populated by officers who manually type information from records into the system. The RMS allows remote access by officers via encrypted, remote sessions – user authenticates via a username and password to search records in the RMS.

Question: Is AA required in this scenario?

USE CASE SCENARIO PANEL

Category: AA

Facts:

- Remote access to CJI
- Remote access from uncontrolled/unknown locations
- Indirect access to CJI
- Username provides identification
- Password provides authentication (something you know)

Answer: No

Since access to the RMS does not provide the ability to run queries or update the CSA, SIB, or national repositories, access to CJI is considered indirect. AA is not required for indirect access to CJI. The user has satisfied the requirement for identification (username) and authentication (password).

USE CASE SCENARIO PANEL

Category: Advanced Authentication (AA)

Scenario #9: Access to CJI stored on a Local Network Drive

Scenario:

The City PD has recently changed its policy to allow remote access (via agency-issued mobile devices - smartphones) to the city RMS. The RMS has connectivity to the state switch and can initiate transactions directly to the state and FBI. The RMS is located within a physically secure location. To access the RMS, the users unlock their phones via PIN (compliant with Section 5.6.2.1.2), then use an encrypted VPN and authenticate to the RMS via a username and password.

Question: Is AA required in this scenario?

USE CASE SCENARIO PANEL

Category: AA

Facts:

- Local network access to CJI
- No remote access
- Direct access to CJI

- Username provides identification
- Password provides authentication (something you know)

Answer: Yes

Users have direct access to CJI via remote access from any location (not restricted to physically secure locations). The user only enters a username and password authenticate to the RMS. The PIN used to unlock the phone is a separate requirement (Section 5.13.7.1 Local Device Authentication) and is not part of the AA solution implemented at the RMS logon stage (CJI access point).

USE CASE SCENARIO PANEL

Category: Personnel Security

Scenario #10: Inmates used for custodial services

Scenario:

The City PD is using inmates from a minimum security prison to perform custodial services for the PD. The inmates conduct custodial services after-hours and are unescorted in areas where CJI may be left unattended or displayed.

Question: Are fingerprint-based background checks required?

USE CASE SCENARIO PANEL

Category: Personnel Security

Facts:

- City PD is a CJA
- Inmates are not performing criminal justice functions
- Inmates have unescorted access to unencrypted CJII via access to open CJII storage areas in a physically secure locations

Answer: Yes

Inmates used to perform custodial services are given unescorted access to unencrypted CJII. The *CJIS Security Policy* does not strictly prohibit those with an arrest history from being authorized for unescorted access to unencrypted CJII, but CSO review and approval is required.

USE CASE SCENARIO PANEL

Category: Personnel Security

Scenario #11: Virtual Escorting for remote CAD maintenance

Scenario:

A County SO is using a private contractor for their Computer Aided Dispatch (CAD). The CAD has connectivity to the state switch and can initiate transactions directly to the state and FBI. The CAD system is maintained by the vendor through remote connections. During each of these remote sessions, the vendors administrator is escorted by authorized CJA personnel in compliance with the *CJIS Security Policy* requirements for virtual escorting of privileged functions (5.5.6 Remote Access).

Question: Are fingerprint-based background checks required?

USE CASE SCENARIO PANEL

Category: Personnel Security

Facts:

- County SO is a CJA
- CAD has direct access to CJI
- Remote access to CJI processing system (CAD)
- Remote access is escorted by authorized personnel

Answer: No

Remote admin personnel are virtually escorted by authorized agency personnel. The remote administrators do not have unescorted access to unencrypted CJI. However, the remote administrative personnel need to be identified and authenticated prior to or during the session. This can be accomplished prior to the session via an AA solution or during the session via active teleconference with the escort throughout the session.

USE CASE SCENARIO PANEL

Category: Personnel Security

Scenario #12: Remote CAD maintenance

Scenario:

A County SO has contracted administrative maintenance service from a well-known vendor for their CAD. The CAD has connectivity to the state switch and can initiate transactions directly to the state and FBI. The CAD system is administered by the vendor through unescorted remote connections. A City PD uses this same vendor for the same service and has already conducted a fingerprint-based record check on these vendor personnel. The SO and PD have signed and executed an interagency agreement for this duty.

Question: Does the SO need to submit fingerprint-based background checks?

USE CASE SCENARIO PANEL

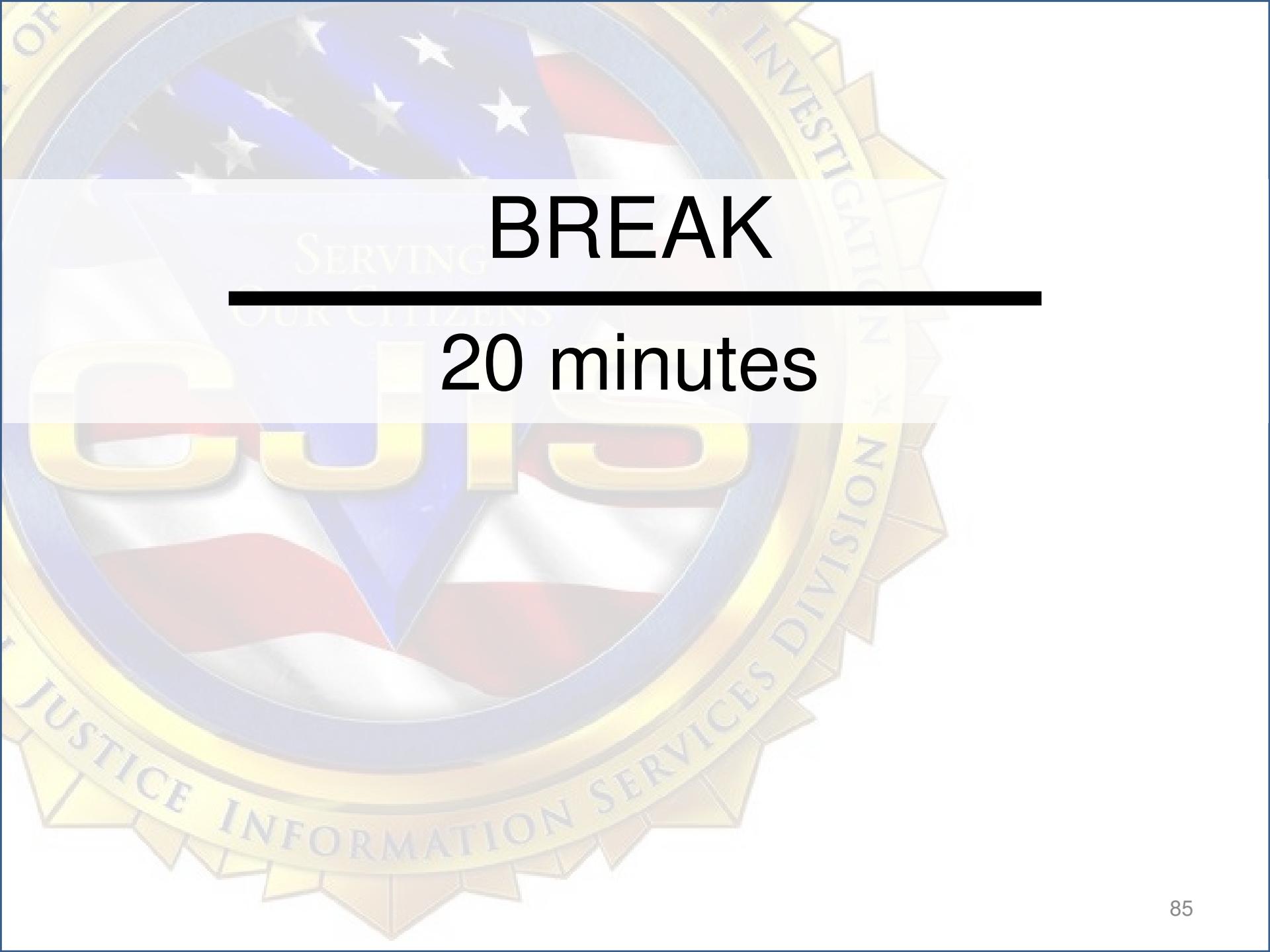
Category: Personnel Security

Facts:

- County SO is a CJA
- City PD is CJA
- CAD has direct access to CJI
- Remote access to CJI processing system (CAD)
- Contractor personnel have unescorted access to unencrypted CJI
- Contractors have been vetted by City PD – in same state as SO

Answer: No

The City PD (same CSO jurisdiction as the County SO) has already performed the proper checks on the vendor personnel and has accepted the responsibility to inform any/all CJAs using this vendor of authorization changes (i.e. If an employee of the vendor is arrested and is no longer allowed access, the Police Department would advise the Sheriff's Office to terminate CJI access for the contractor.).

A faint watermark of the Federal Bureau of Investigation seal is visible in the background. The seal features a shield with stars and stripes, surrounded by a circular border with the words "DEPARTMENT OF JUSTICE", "FEDERAL BUREAU OF INVESTIGATION", and "SPECIAL AGENT".

BREAK

20 minutes

USE CASE SCENARIO PANEL

Category: Personnel Security (NCJA)

Scenario #13: Fingerprint-based record checks for nurse licensing

Scenario:

The Board of Nursing (BoN) is submitting fingerprint-based record checks for the licensing of nurses under an FBI-approved state statute (Public Law 92-544). Since many of the internal BoN employees will have access to CHRI received from these checks, the agency is also conducting fingerprint collection and submission of internal staff for records checks under this statute.

Question: Is the NCJA in compliance?

USE CASE SCENARIO PANEL

Category: Personnel Security (NCJA)

Facts:

- BoN is a NCJA
- The state has a Public Law 92-544 statute in place
- PL 92-544 permits submission of fingerprints for records check for the purpose of nurse licensure
- PL 92-544 does not address internal BoN employee fingerprint records checks

Answer: No

In this scenario the state statute does not include authorization to fingerprint for “access to CHRI.” Unless specifically stated, CHRI can only be obtained with authorization and used for the purpose of which it was obtained (i.e., check completed for licensure of board members).

USE CASE SCENARIO PANEL

Category: Personnel Security (NCJA)

Scenario #14: Fingerprint-based record checks for teacher licensing

Scenario:

The Department of Education (DoE) is submitting fingerprint-based record checks for the licensing of teachers under an FBI-approved state statute (Public Law 92-544). The statute does not stipulate that any additional collection and submission of fingerprints for record checks, such as internal staff employment is authorized. The DoE is not fingerprinting internal staff who process the licensure for teachers.

Question: Is the NCJA in compliance?

USE CASE SCENARIO PANEL

Category: Personnel Security (NCJA)

Facts:

- DoE is a NCJA
- The state has a Public Law 92-544 statute in place
- PL 92-544 permits submission of fingerprints for records check for the purpose of teacher licensure
- PL 92-544 does not address internal DoE employee fingerprint records checks

Answer: Yes

An NCJA is only authorized to submit a fingerprint-based record check when authority to do so exists. Because the statute does not authorize fingerprint-based record checks for DoE employees, the agency is not authorized to submit additional fingerprints of internal staff personnel for record checks.

USE CASE SCENARIO PANEL

Category: Outsourcing Noncriminal Justice Functions

Scenario #15: Outsourcing NCJA network access to CJI

Scenario:

The DoE is submitting fingerprint-based record checks for the licensing of teachers under an FBI-approved state statute (Public Law 92-544). The DoE is defined within the statute as the authorized recipient (AR). When the CHRI results are returned from the CSA, the DoE saves the .pdf file containing the CHRI results on a network file share maintained by the State Department of Information Technology (DoIT).

Question: Is the NCJA in compliance?

USE CASE SCENARIO PANEL

Category: Outsourcing Noncriminal Justice Functions

Facts:

- DoE is a NCJA
- The state has a Public Law 92-544 statute in place
- DoE is the authorized recipient
- DoE puts CJI (CHRI) on network file share
- Network file share is operated by DoIT
- DoIT personnel would have access to CJI

Answer: No

Any non-AR personnel performing services granting unescorted access to unencrypted CJI is ‘outsourcing’. The Security and Management Control Outsourcing Standard for Non-Channelers (Outsourcing Standard) requires prior approval, in writing, from the State Compact Officer/Chief Administrator in order for the AR (DoE) to outsource.

USE CASE SCENARIO PANEL

Category: Outsourcing Noncriminal Justice Functions

Scenario #16: Outsourcing contractor administrative access to CJI

Scenario:

The Department of Health and Welfare (DHW) is submitting fingerprint-based record checks for licensing under an FBI-approved state statute (Public Law 92-544). The DHW is defined within the statue as the authorized recipient (AR). The DHW is saving the CJI (CHRI) responses in a SQL database and emailing CJI to the individual of record. A private contractor is providing the SQL and email IT services. The DHW has received verbal permission from the State Compact Officer to permit contractor personnel unescorted access to unencrypted CJI.

Question: Is the NCJA in compliance?

USE CASE SCENARIO PANEL

Category: Outsourcing Noncriminal Justice Functions

Facts:

- DHW is a NCJA
- The state has a Public Law 92-544 statute in place
- DHW is the authorized recipient
- SQL and email services are outsourced to private contractor
- State Compact Officer gave verbal permission for outsourcing

Answer: No

Although the State Compact Officer approved outsourcing, the approval was not provided in writing for verification during the audit.

USE CASE SCENARIO PANEL

Category: Outsourcing Noncriminal Justice Functions

Scenario #17: Outsourcing cloud-based email service (Office365)

Scenario:

The Department of Children and Family Services (DCFS) is submitting fingerprint-based record checks on personnel with access to children under a FBI-approved state statute (Public Law 92-544). DCFS is defined within the statue as the AR. DCFS employees are emailing the CHRI results to other DCFS employees throughout the state. The emails are encrypted in transit (FIPS 140-2 certified, 128 bit symmetric algorithm) using the option in Office365.

Question: Is the NCJA in compliance?

USE CASE SCENARIO PANEL

Category: Outsourcing Noncriminal Justice Functions

Facts:

- Department of Children and Family Services is a NCJA
- The state has a Public Law 92-544 statute in place
- Department of Children and Family Services is the AR
- Email and encryption service provided by Microsoft Office 365
- No outsourcing permission given

Answer: No

Although the emails are encrypted, contractor personnel of Microsoft are providing encryption services, which gives them administrative access to the key infrastructure allowing unescorted access to unencrypted CJI. The AR has not obtained prior approval for outsourcing (unescorted access to unencrypted CJI by Microsoft personnel to provide encryption service).

USE CASE SCENARIO PANEL

Category: Mobile Device Management (MDM)

Scenario #18: Web Portal access

Scenario:

The CSA is using a web-based application to distribute CJI to noncriminal justice agencies authorized to receive CHRI for employment or licensing. The application is internet-based and is accessible from any internet connection. The user is required to authenticate to the application (using AA) which enforces a secure, encrypted (FIPS 140-2 certified, 128 bit symmetric algorithm) connection. The CSA does permit web access from mobile devices with limited-feature operating systems.

Question: Is the use of an MDM required on these mobile devices?

USE CASE SCENARIO PANEL

Category: MDM

Facts:

- CSA is a CJA
- CSA maintains a web portal used to distribute CJI (CHRI) – direct access to CJI
- Access to the web is remote connection – AA is used
- Mobile devices can be used to retrieve CJI from the web
- Mobile device using limited-feature OS are permitted access

Answer: Yes

CJI is accessible from any internet connection via the web portal. Mobile devices with limited-feature operation systems that access unencrypted CJI are required to utilize MDMs (as required in Section 5.13.2) to access CJI.

USE CASE SCENARIO PANEL

Category: Mobile Device Management (MDM)

Scenario #19: Microsoft Surface remote connection to local RMS

Scenario:

A City PD has recently issued Microsoft Surface tablets which run the Windows 10 Operation System. These tablets are used to remotely access the agency's local RMS. The RMS does not have connectivity to any state or federal system to perform transactional queries, but contains CJI. Remote connectivity to the RMS is required to use an encrypted VPN connection (FIPS 140-2 certified, 128 bit symmetric algorithm). The agency requires the use of AA for all remote connections.

Question: Is the use of an MDM required on these mobile devices?

USE CASE SCENARIO PANEL

Category: MDM

Facts:

- City PD is a CJA
- Remote access to RMS – indirect access to CJI
- Mobile device is used – tablet
- Tablet uses Windows 10 (full-feature operation system)

Answer: No

The requirement for MDM only applies to mobile devices that run limited-feature operating systems. The Microsoft Surface used to remotely access the local RMS utilizes a full-feature operating system and has the ability (and requirement) to comply with Sections 5.10.4.2 Malicious Code Protection and 5.13.4.3 Personal Firewall.

USE CASE SCENARIO PANEL

Category: Mobile Device Management (MDM)

Scenario #20: iPad remote connection to county RMS

Scenario:

A County SO has recently issued iPad tablets which run the latest version of iOS. These tablets are used to remotely access the county RMS. The RMS has connectivity to state and federal systems and can perform transactional queries to get CJI. Remote connectivity to the RMS is required to use an encrypted VPN connection (FIPS 140-2 certified, 128 bit symmetric algorithm). The agency requires the use of AA for these remote connections.

Question: Is the use of an MDM required on these mobile devices?

USE CASE SCENARIO PANEL

Category: MDM

Facts:

- County SO is a CJA
- Remote access to RMS – direct access to CJIS
- Mobile device is used – tablet
- Tablet uses iOS (limited-feature operation system)

Answer: Yes

The iPad uses a limited-feature operating system and accesses CJIS. Therefore, it must comply with Section 5.13.2 Mobile Device Management.

Wrap Up & Closing Remarks

George White

FBI CJIS Information Security Officer