ISO Symposium

August 20, 2014

FBI CJIS Information Security Officer Program Office

iso@leo.gov

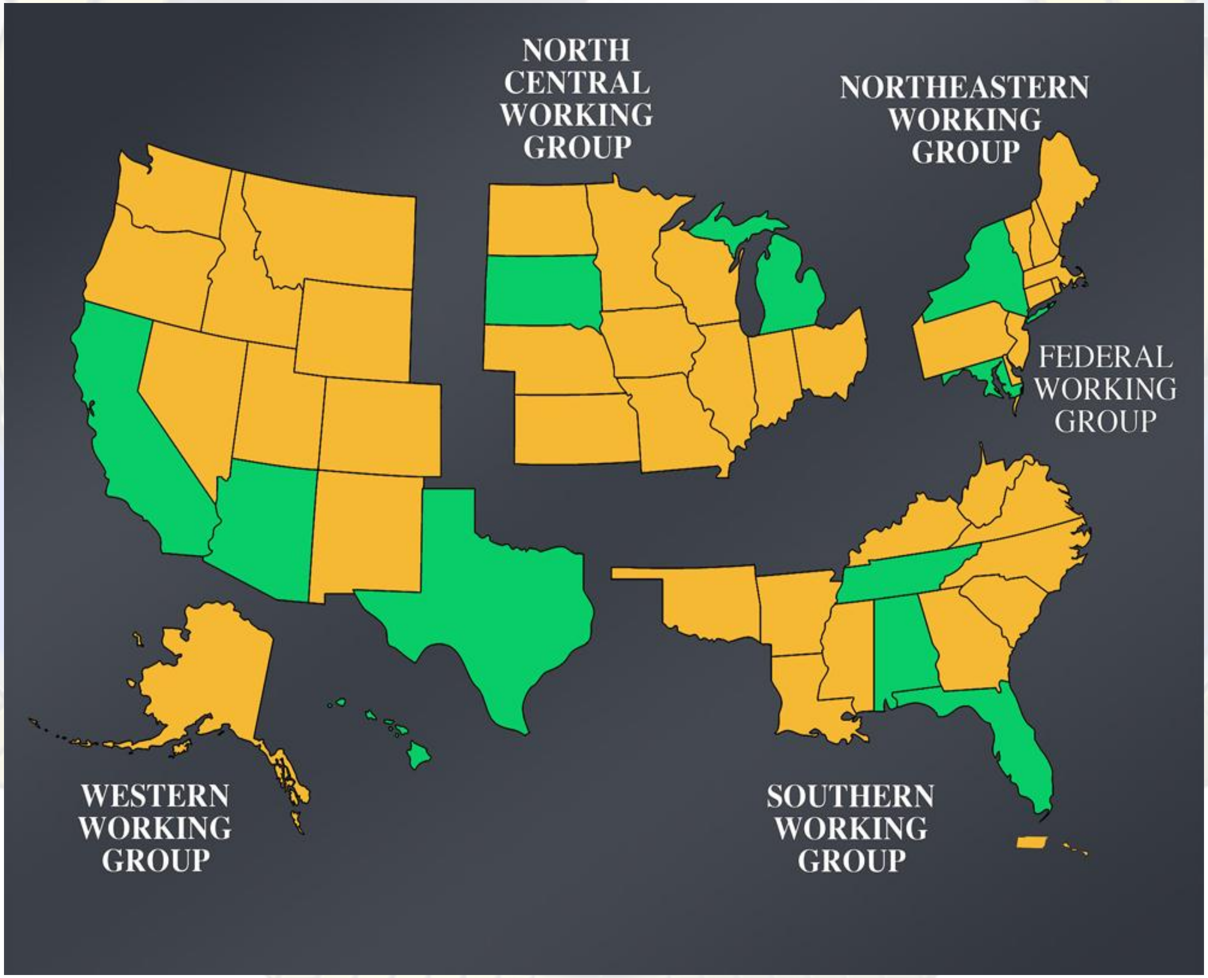
Introductions

George White

Chief, CJIS Information Assurance Unit

FBI CJIS Information Security Officer

SECURITY AND ACCESS SUBCOMMITTEE



Representation:

Chairman: Alan Ferretti – TX, DPS

Vice Chair: Jeff Matthews – AL, CJIC

Brenda Abaya – HI, CJDC

Larry Coffee – FL, FDLE

Joe Dominic – CA, DOJ

Troy Goodman – MD, DPS

Blaine Koops – MI, Sheriff of Allegan County

Yosef Lehrman – NY, NYPD Network Ops

Bill Phillips – AZ, NLETS

Charles Shaffer – FL, FDLE (Compact Rep)

TJ Smith – CA, LASD

Delton Tipton – SD, LETS

Brad Truitt – TN, BOI

ISO Symposium Presenters

FBI CJIS Audit Staff:

Mike McIntyre, Supervisory IT Specialist

Candice Preston, IT Specialist/Systems Auditor

Russell Myers, IT Specialist/Systems Auditor

Ronnie George, Management and Program Analyst

FBI CJIS ISO Program Staff:

George White, FBI CJIS ISO

Jeff Campbell, Assistant ISO

Lora Klingensmith, Sr. Management and Program Analyst

Steve Exley, Sr. Technical Analyst

Announcements

- There will be a Happy Hour tonight from 5:30pm-? Sponsored by Diverse Computing, Inc. This will be held at the Bluegrass Brewing Co. 300 West Main Street.

  Everyone is welcome to attend.

- Peer-to-Peer session tonight from 7-9pm in this room for ISO's only. Sign up for topic recommendation located in the back of the room.

- ISO Trivia

Opening Remarks

Stephen Morris

Assistant Director, FBI CJIS Division

Housekeeping

- Please place cell phones/pagers/iPads and anything else with a ringer on vibrate as to not disrupt the symposium presenters.
- Breaks will be:
  - 10:30am (on you)
  - 12:00pm Lunch (on you)
  - 2:30pm (snacks and drinks will be served)
- The sign-in sheet will be passed around the room. Please check your information and make any necessary corrections.
- If you do not get the sign in sheet or are somehow bypassed please see me.
- If you need changes in travel, please see one of the CJIS ladies at the registration desk.

Housekeeping

- Please obtain your ORIGINAL hotel receipt and ensure there is a $0 balance.

- Please be sure to send all original receipts, along with your voucher in the packet you received at the Registration Desk. Do not send back restaurant receipts, we don't need those. If you are being reimbursed but have not picked up your packets, or need to change your banking information, stop by the Registration Desk and see Kathy Oldaker.

- You will not receive a copy of the Symposium PowerPoint presentations. If you are interested in an electronic copy please complete the presentation request form and return to Kathy Oldaker or Registration Desk.

Housekeeping

- Stump the ISO (Open Forum) question submission cards will be located in the back of the room – please fill one out and place in the basket.

- We will have microphones available throughout the symposium for questions – if you want to ask the presenter a question raise your hand and we will get the microphone to you as quickly as possible.

- Surveys – Morning and Afternoon. Feedback is greatly appreciated. Please fill out and leave on your table for collection.

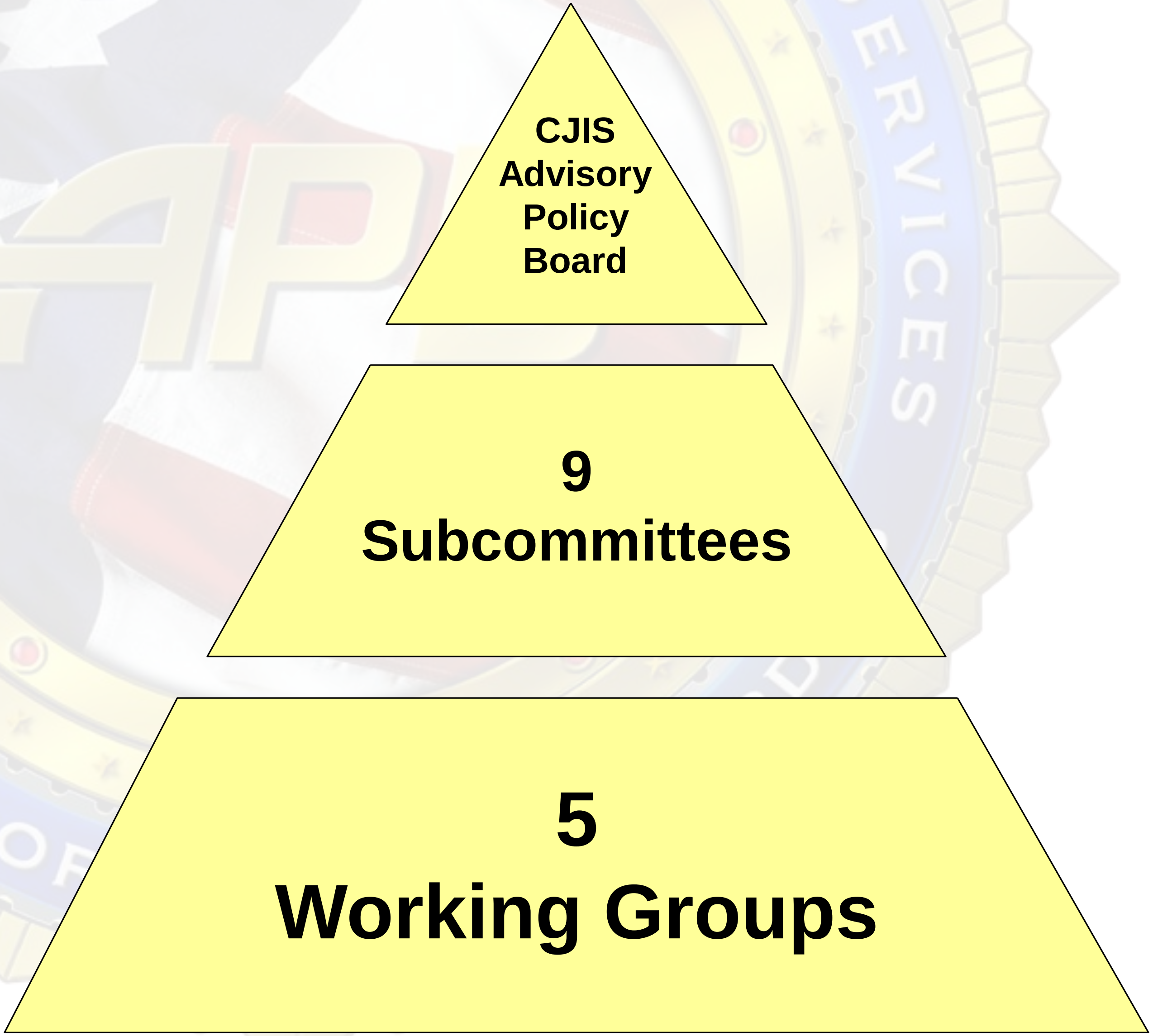
- Have a GREAT Symposium

CJIS Security Policy Version 5.3 Changes

Jeff Campbell

FBI CJIS Assistant Information Security Officer

CJIS ADVISORY PROCESS

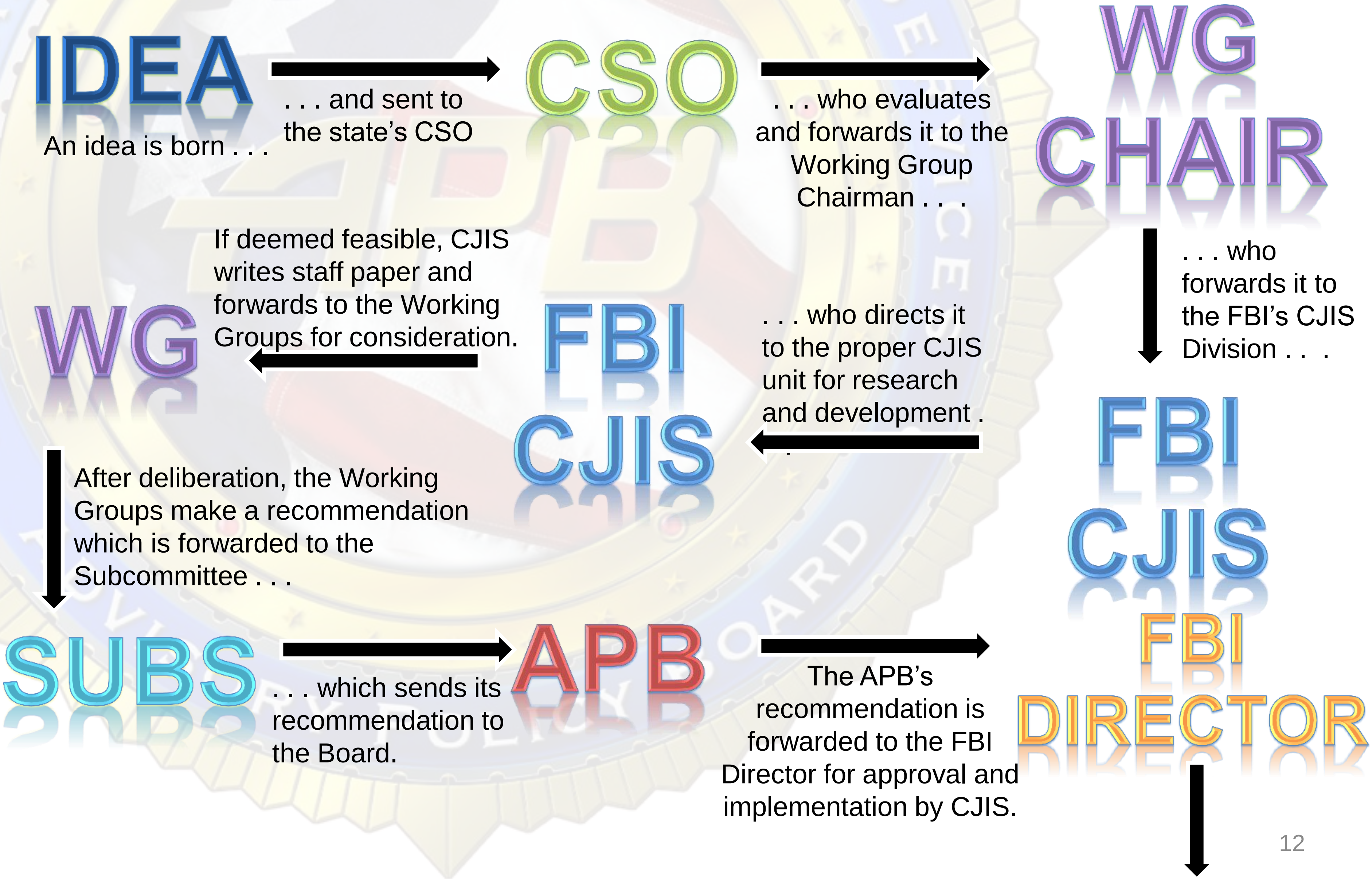


CJIS Advisory Policy Board

9 Subcommittees

5 Working Groups

CJIS ADVISORY PROCESS



IDEA

An idea is born . . .

. . . and sent to the state's CSO

CSO

. . . who evaluates and forwards it to the Working Group Chairman . . .

WG CHAIR

. . . who forwards it to the FBI's CJIS Division . . .

FBI CJIS

. . . who directs it to the proper CJIS unit for research and development .

FBI CJIS

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

WG

After deliberation, the Working Groups make a recommendation which is forwarded to the Subcommittee . . .

SUBS

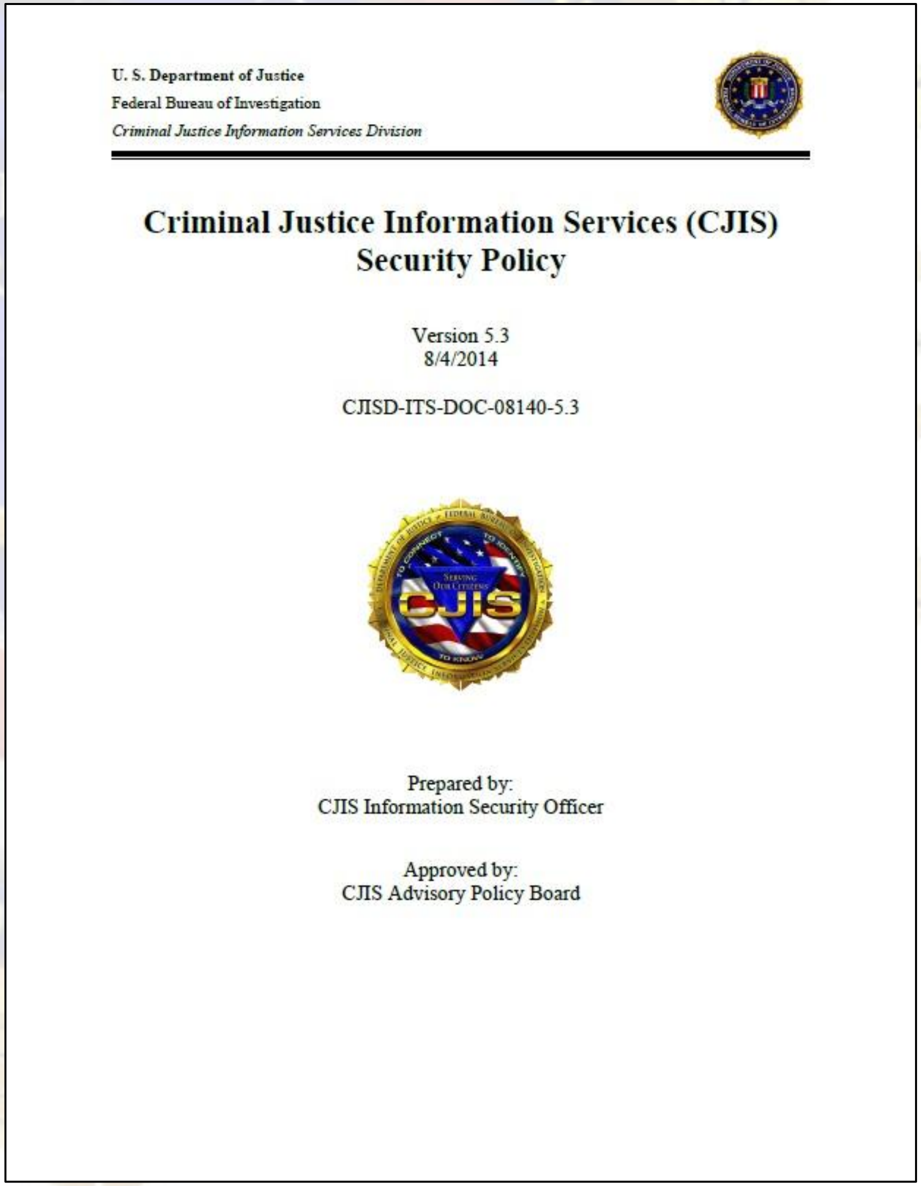
. . . which sends its recommendation to the Board.

APB

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

FBI DIRECTOR

CJIS ADVISORY PROCESS



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

Criminal Justice Information Services (CJIS) Security Policy

Version 5.3
8/4/2014

CJISD-ITS-DOC-08140-5.3

Prepared by:
CJIS Information Security Officer

Approved by:
CJIS Advisory Policy Board

SIGNIFICANT CHANGES FOR v5.3

- Annual release cycle
- July / August Time Frame
- Incorporates APB approved changes from previous year (2 cycles: Spring / Fall)
- Incorporates administrative changes

SIGNIFICANT CHANGES FOR v5.3

Section 4.2.2 Proper Access, Use, and Dissemination of NCIC Restricted Files Information

- Add these files:

  Violent Person File
  NICS Denied Transaction File

- Remove this file:

  Immigration Violator File

SIGNIFICANT CHANGES FOR v5.3

Sections 5.6.2.2.1 Advanced Authentication Policy and Rationale

- Removal of the ***INTERIM COMPLIANCE*** for advanced authentication (AA)
- Addition of ***COMPENSATING CONTROLS*** for AA on smartphones and tablets
- Remove requirement for AA for ***INDIRECT ACCESS***
- Change decision tree accordingly

SIGNIFICANT CHANGES FOR v5.3

Removal of the ***INTERIM COMPLIANCE*** for advanced authentication (AA)

- Set to expire on Sept. 30, 2014
- For AA purposes, police vehicle = physically secure location
- Devices associated with and located within a police vehicle
- IPSec for AA will expire on Sept. 30, 2014

SIGNIFICANT CHANGES FOR v5.3

Addition of ***COMPENSATING CONTROLS*** for AA

- Applies only to smartphones and tablets
- Possession of agency issued device is a required part of control
- Additional requirements mostly met by MDM
- Compensating Controls are temporary
- CSO approval and support required

SIGNIFICANT CHANGES FOR v5.3

Addition of ***COMPENSATING CONTROLS*** for AA

- Meet the intent of the CJIS Security Policy AA requirement
- Provide a similar level of protection or security as the original AA requirement
- Not rely upon existing requirements for AA as compensating controls

SIGNIFICANT CHANGES FOR v5.3

Remove requirement for AA for ***INDIRECT ACCESS***

- Add ***DIRECT or INDIRECT ACCESS*** as a "determiner" for advanced authentication (AA)
- No ability to conduct transactional activities on state and national repositories
- CSO determines whether access is considered indirect

SIGNIFICANT CHANGES FOR v5.3

Appendix A: Create definition of ***INDIRECT ACCESS***

“Having the authority to access systems containing CJI without providing the user the ability to conduct transactional activities (the capability to query or update) on state and national systems (e.g. CJIS Systems Agency (CSA), State Identification Bureau (SIB), or national repositories).”

SIGNIFICANT CHANGES FOR v5.3

Section 5.5.5 Session Lock

- Exemption for receive-only terminals

“(3) terminals designated solely for the purpose of receiving alert notifications (i.e. receive only terminals or ROT) used within physically secure location facilities that remain staffed when in operation.”

SIGNIFICANT CHANGES FOR v5.3

Section 5.6.2.1.2 Personal Identification Number

- Addition of PIN requirements
- When used as authenticator must meet password requirements
- Local device authentication – 6 digits
- When used in conjunction with a certificate or token, use the following attributes

SIGNIFICANT CHANGES FOR v5.3

Be a minimum of six (6) digits
Have no repeating digits (i.e., 112233)
Have no sequential patterns (i.e., 123456)
Not be the same as the Userid.
Expire within a maximum of 365 calendar days.

> *If a PIN is used to access a soft certificate which is the second factor of authentication, AND the first factor is a password that complies with the requirements in Section 5.6.2.1.1, then the 365 day expiration requirement can be waived by the CSO.*

Not be identical to the previous three (3) PINs.
Not be transmitted in the clear outside the secure location.
Not be displayed when entered.

EXCEPTION: When a PIN is used for local device authentication, the only requirement is that it be a minimum of six (6) digits.

SIGNIFICANT CHANGES FOR v5.3

Section 5.9.1 Physically Secure Location

- "A physically secure location is a facility, ***a police vehicle,*** or an area, a room, or a group of rooms within a facility with both the physical and personnel security controls sufficient to protect CJI and associated information systems."

- Removal of the ***INTERIM COMPLIANCE*** for police vehicle and advanced authentication (AA)

SIGNIFICANT CHANGES FOR v5.3

SIGNIFICANT CHANGES FOR v5.3

SIGNIFICANT CHANGES FOR v5.3

Section 5.10.1.2 Encryption

- CJI at rest exception
- Create passphrase requirements
  - Used for encryption **NOT** authentication
  - Different requirements than passwords
- File versus folder use

SIGNIFICANT CHANGES FOR v5.3

Section 5.10.1.2 Encryption

- Create encryption exception for CJI at rest

“EXCEPTION: When encryption is used for CJI at rest, agencies may use encryption methods that are FIPS 197 certified, AES 256 bit as described on the National Security Agency (NSA) Suite B Cryptography list of approved algorithms.”

SIGNIFICANT CHANGES FOR v5.3

- NIST cryptographic algorithms approved by NSA

Algorithm	**Function**	**Specification**	**Parameters**
Advanced Encryption Standard (AES)	***Symmetric block cipher used for information protection***	***FIPS PUB 197 (reference g.)***	***Use 128 bit keys to protect up to SECRET.*** ***Use 256 bit keys to protect up to TOP SECRET.***
Elliptic Curve Diffie-Hellman (ECDH) Key Exchange	Asymmetric algorithm used for key establishment	NIST SP 800-56A (reference h.)	Use Curve P-2561 to protect up to SECRET. Use Curve P-384 to protect up to TOP SECRET.
Elliptic Curve Digital Signature Algorithm (ECDSA)	Asymmetric algorithm used for digital signatures	FIPS PUB 186-3 (reference f.)	Use Curve P-256 to protect up to SECRET. Use Curve P-384 to protect up to TOP SECRET.
Secure Hash Algorithm (SHA)	Algorithm used for computing a condensed representation of information	FIPS PUB 180-4 (reference e.)	Use SHA-256 to protect up to SECRET. Use SHA-384 to protect up to TOP SECRET.

SIGNIFICANT CHANGES FOR v5.3

- Legacy NIST cryptographic algorithms approved by NSA

Algorithm	Function	Specification	Parameters
Diffie-Hellman (DH) Key Exchange	Asymmetric algorithm used for key establishment	NIST SP 800-56A (Reference h.)	Use 2048 bit modulus to protect up to SECRET.
Digital Signature Algorithm (DSA)	Asymmetric algorithm used for digital signatures	FIPS PUB 186-3 (reference f.)	Use 2048 bit modulus to protect up to SECRET.
RSA	Asymmetric algorithm used for digital signatures	FIPS PUB 186-3 (reference f.)	Use 2048 bit modulus to protect up to SECRET.

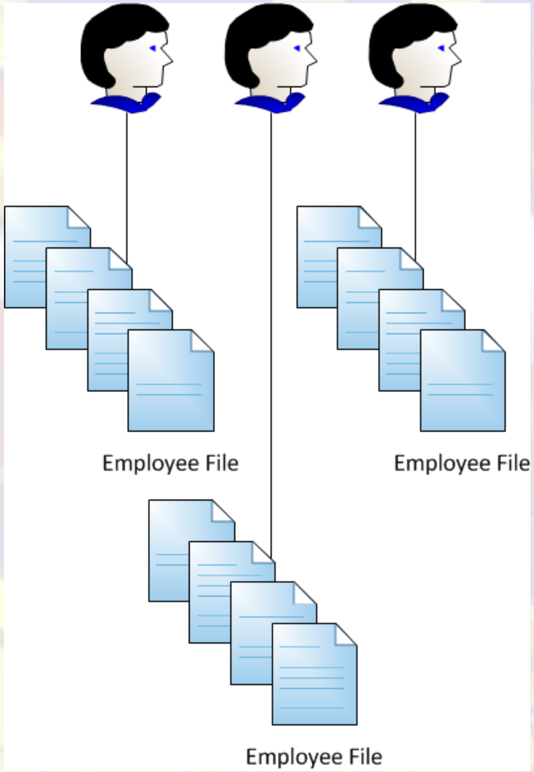
SIGNIFICANT CHANGES FOR v5.3

When agencies implement encryption on CJI at rest, the passphrase used to unlock the cipher shall meet the following requirements:

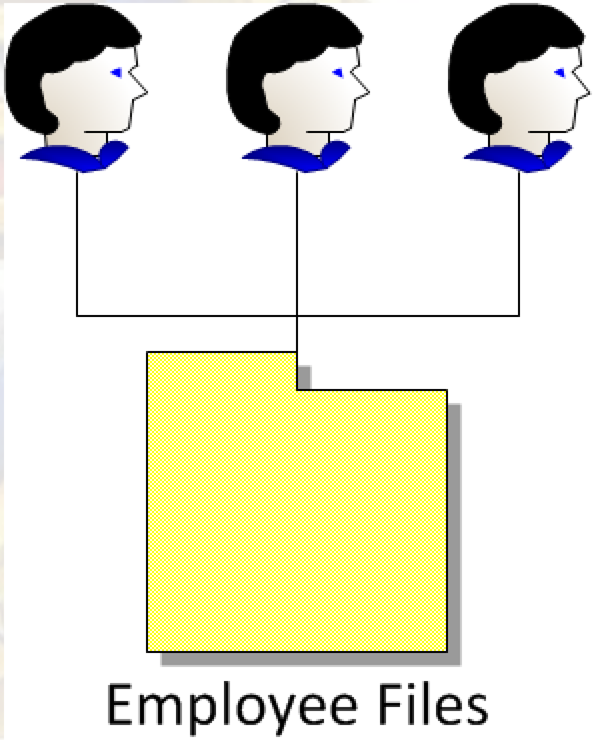
- ***Be at least 10 characters***
- ***Not be a dictionary word.***
- ***Include at least one (1) upper case letter, one (1) lower case letter, one (1) number, and one (1) special character.***
- ***Be changed when previously authorized personnel no longer require access.***

SIGNIFICANT CHANGES FOR v5.3

File Versus Folder Use



Individual Passphrases



Single Shared Passphrase

SIGNIFICANT CHANGES FOR v5.3

NEW: Policy area 5.13 Mobile Devices

- Consolidation of mobile centric requirements
- Reference to “companion” sections
- New requirements

SIGNIFICANT CHANGES FOR v5.3

Appendix A Terms and Definitions

- Mobile device form factors
  - Pocket/handheld mobile devices
  - Smartphone
  - Tablet Devices
- Indirect Access
- Digital Media
- Receive-only terminal

SIGNIFICANT CHANGES FOR v5.3

Questions?

Personnel Access and Security Requirements

George White

FBI CJIS ISO

PERSONNEL ACCESS & SECURITY REQUIREMENTS

- **Types of CJI Access**
- **Physical Protection**
- **Security Awareness Training**
- **Personnel Security**
- **Scenarios**

PERSONNEL ACCESS & SECURITY REQUIREMENTS

Types of CJI Access

PERSONNEL ACCESS & SECURITY REQUIREMENTS

Types of CJI Access

- Type of access drives applied requirements
  - Logical Access
  - Physical Access
  - Direct Access
  - Indirect Access
- Access refers to the capability, not necessarily the act
- All access types require security awareness training some require background checks

Types of CJI Access

Physical Access i.e. “Walkin’ ‘round access”

- Defined by the CJIS Security Policy as:

  The physical ability, right or privilege to view, modify or make use of CJI by means of physical presence within the proximity of computers and network devices (e.g. the ability to insert a boot disk or other device into the system, make a physical connection with electronic equipment, etc.).

- A person within physical proximity of CJI or CJI processing systems who may view, modify, or make use of CJI has physical access.

PERSONNEL ACCESS & SECURITY REQUIREMENTS

Types of CJI Access

Logical Access

- Defined by the CJIS Security Policy as:

  The technical means (e.g., read, create, modify, delete a file, execute a program, or use an external connection) for an individual or other computer system to utilize CJI or CJIS applications.

- A person logging into a system/network/application (even remotely) with the ability to gain access to CJI has logical access.

Types of CJI Access

Direct Access

- Defined by the CJIS Security Policy as:

  1) *Having the authority to access systems managed by the FBI CJIS Division, whether by manual or automated methods, not requiring the assistance of, or intervention by, any other party or agency (28 CFR, Chapter 1, Part 20).*
  2) *Having the authority to query or update national databases maintained by the FBI CJIS Division including national queries and updates automatically or manually generated by the CSA.*

- A person with the ability to query or update the national databases directly or through the CSA has direct access.

Types of CJI Access

Indirect Access

- Defined by the CJIS Security Policy as:

  Having the authority to access systems (i.e., repository, application, or service) containing CJI that do not provide the user the ability to conduct transactional activities (the capability to query or update) on state and national systems (i.e., CJIS Systems Agency (CSA), State Identification Bureau (SIB), or national repositories).

- User can query a local database populated by static copies of CJI
- No direct connectivity to query or send updates to state and national databases

PERSONNEL ACCESS & SECURITY REQUIREMENTS

Types of CJI Access

Physical or Logical Access or Both?

- Determines what level of security awareness is required

Direct or Indirect Access?

- Determine if Advanced Authentication (AA) would be required for remote access
- Fingerprint-based background checks are required for direct access to CJI
- Conversely, background checks may not be required for indirect access to CJI

PERSONNEL ACCESS & SECURITY REQUIREMENTS

Physical Protection

PERSONNEL ACCESS & SECURITY REQUIREMENTS

Physical Protection

Physical Protection Policy and Procedures

- CJIS Security Policy Section 5.9:

  Physical protection policy and procedures shall be documented and implemented to ensure CJI and information system hardware, software, and media are physically protected through access control measures.

- Protect CJI through physical access control

PERSONNEL ACCESS & SECURITY REQUIREMENTS

Physical Protection

Physically Secure Location

- APB-approved definition change in CJIS Security Policy v5.3:

  *A facility, **a police vehicle**, or an area, a room…*

- A physically secure location environment permits the "open storage" of CJI – no encryption requirement
  - ➢ Presents potential for physical access to CJI
  - ➢ Security awareness training required for unescorted access

PERSONNEL ACCESS & SECURITY REQUIREMENTS

Physical Protection

Controlled Area

- Required when an agency (CJA or NCJA) has an operational need to access or store CJI, but cannot meet all of the physical, personnel, and technical controls required for establishing a physically secure location
- An area, a room, or a storage container used for CJI access or storage
  - ➢ Limit access during CJI processing only to authorized personnel
  - ➢ Lock the area, room, or storage container when unattended
  - ➢ Prevent CJI access and viewing from unauthorized individuals
  - ➢ Encrypt CJI at rest in accordance with Section 5.10.1.2

PERSONNEL ACCESS & SECURITY REQUIREMENTS

Physical Protection

Encryption

Required:

- ✓ CJI is transmitted outside the boundaries of a physically secure location *(FIPS 140-2 certified, 128 bit)*
- ✓ CJI at rest outside of physically secure locations *(NSA Suite B, 256 bit or FIPS 140-2 certified, 128 bit)*
- ✓ CJI at rest within controlled areas *(AES, 256 bit)*

Not required:

- x CJI transmitted within a physically secure location
- x CJI at rest within a physically secure location

Physical Protection

Escorting

- In physically secure locations, unauthorized users and visitors must be escorted for access
- Authorized personnel must accompany and monitor unauthorized personnel, but must also be able to intervene when/if necessary to prevent unauthorized actions
- The use of cameras or other electronic means used to monitor a physically secure location does not constitute an escort

PERSONNEL ACCESS & SECURITY REQUIREMENTS

Physical Protection

Advanced Authentication (AA)

Required:

✓ When requesting access to unencrypted CJI from outside the boundaries of a physically secure location (e.g., remote access)

Or

✓ Technical security requirements for a physically secure location have not been met

Not required:

x When requesting access to CJI from within the perimeter of a physically secure location

And

x The technical security controls have been met

Or

x User has indirect access CJI

PERSONNEL ACCESS & SECURITY REQUIREMENTS

Physical Protection

Who is responsible for Physical Protection?

- The physically secure location is subject to information exchange agreements, criminal justice agency management control; SIB control; FBI CJIS Security Addendum; or a combination thereof and may be audited by both the CSA and FBI.
- Everyone in the facility is responsible for Physical Protection… educate, educate, educate!

PERSONNEL ACCESS & SECURITY REQUIREMENTS

Security Awareness Training

PERSONNEL ACCESS & SECURITY REQUIREMENTS

Security Awareness Training

When is Security Awareness Training Required?

- All personnel within six (6) months of initial assignment receive training
- Biennially thereafter

Note: The CSO/SIB has discretion to accept security awareness training documentation from another agency

Three “Levels” of Training (determined by role):

1. All Personnel (generalized training) – “Level” 1 Only
2. Personnel with Physical and Logical Access (CJI processing) – 1+2
3. Personnel with Technology Roles (administrator roles) – 1+2+3

PERSONNEL ACCESS & SECURITY REQUIREMENTS

Security Awareness Training

Who Needs Security Awareness Training?

- All CJA and NCJA employees with the need for continuous access to CJI (physical, logical, direct, or indirect) to perform their job

Who Does Not Need Security Awareness Training?

- Limited access to CJI controlled via escort for a special scenario (e.g., equipment installation in a server room or a ride-along) may provide an exception, if permitted by the agency

PERSONNEL ACCESS & SECURITY REQUIREMENTS

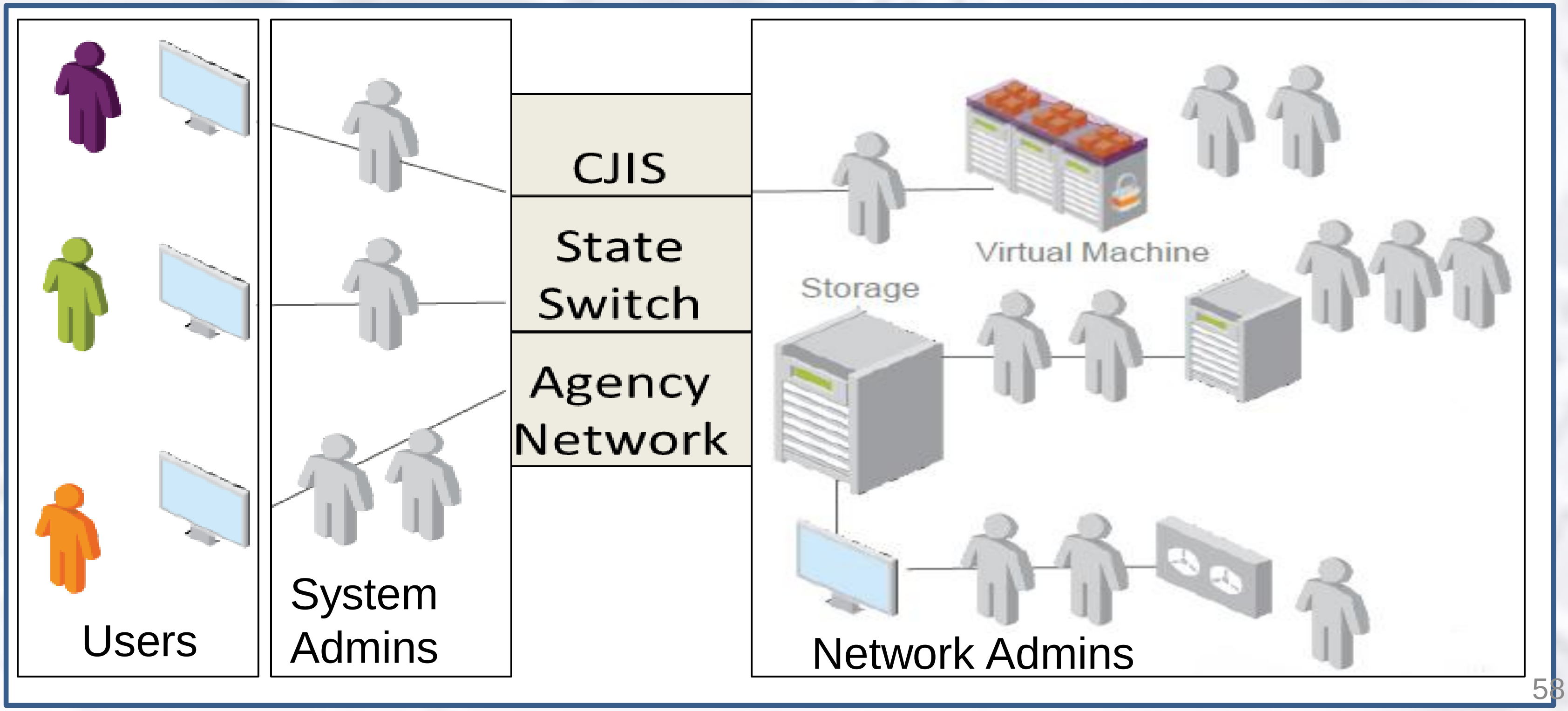
Personnel Security

PERSONNEL ACCESS & SECURITY REQUIREMENTS

Personnel Security

Personnel Security

- Where statutory or administrative authority allows - Section 5.12 applies to ALL personnel who have unescorted access to CJI



PERSONNEL ACCESS & SECURITY REQUIREMENTS

Personnel Security

Personnel Security Policy and Procedures

- State of residency and national fingerprint-based background checks for all personnel with direct access to CJI
  - Within 30 days of assignment
  - Contractors and vendors prior to CJI access
- Reinvestigations recommended every five (5) years unless Rap Back is implemented
- The CSO, or designee*, determines CJI access based on the results of the background checks

** Note: All CSO designees shall be from an authorized criminal justice agency.*

PERSONNEL ACCESS & SECURITY REQUIREMENTS

Personnel Security

Background Checks for NCJAs

- Section 5.12 applies to agencies located within states having passed legislation authorizing or requiring civil fingerprint-based background checks for personnel with access to criminal history record information for the purposes of licensing or employment
- Agencies located within states without authorizing legislation or authority are exempted from the fingerprint-based background check requirement until such time as appropriate legislation has been written into law
- Exemption does NOT apply to CJAs!

PERSONNEL ACCESS & SECURITY REQUIREMENTS

Personnel Security

Personnel Termination

- Upon termination of individual employment, immediately terminate access to CJI.

Personnel Transfer

- The agency shall review the CJI access authorizations when personnel are reassigned or transferred to other positions.

Personnel Sanctions

- Employ a formal sanctions process for personnel failing to comply with policies and procedures.

PERSONNEL ACCESS & SECURITY REQUIREMENTS

Scenarios

PERSONNEL ACCESS & SECURITY REQUIREMENTS

Scenarios

So, how do I determine what the requirements for permitting CJI access to an individual?

- What type of CJI access does the user have?
  - ❑ Physical, Logical, Admin? (Security Awareness)
  - ❑ Direct or Indirect? (Background Checks, AA)
- What is the user's location? (Background Checks, Encryption, AA)
  - ❑ Physically secure location, controlled area, remote location?
- What is the data's location? (Encryption)
  - ❑ Physically secure location, controlled area, remote location?

PERSONNEL ACCESS & SECURITY REQUIREMENTS

Scenarios

Scenario #1:

An officer arrests an individual and runs an NCIC check from an MDT "hard mounted" within his police vehicle.

- The officer has direct, physical, and logical access to CJI –
  - ✓ Conduct background check and "level 2" security awareness training (personnel with physical and logical access)
- The NCIC query and return CJI traverses an encrypted VPN (FIPS 140-2 certified, 128 bit) between the police vehicle and PD (both physically secure locations)
  - ✓ AA is not required
  - ✓ Encryption is not required for CJI at rest

PERSONNEL ACCESS & SECURITY REQUIREMENTS

Scenarios

Scenario #2:

An NCJA employee is converting hard copy files including employee background check information into digital documents, then storing the file in a local RMS database for local HR access.

- The user has physical, logical, and indirect access to static CJI
  - ✓ Receive "level 2" security awareness training (personnel with physical and logical access)
  - ✓ No background check is required for indirect access
  - ✓ AA is not required
- The CJI is stored in a shared drive on the NCJA network
  - ✓ Encryption is required for CJI at rest (Section 5.10.1.2)

PERSONNEL ACCESS & SECURITY REQUIREMENTS

Scenarios

FAQ #1:

Question:
We have a consolidated server room shared amongst multiple departments. These departments have administrative personnel (not background checked) that need access to do maintenance work on their servers. All CJI in transit and at rest within the server room is encrypted (FIPS 140-2 certified, 128 bit). Must the server room be a physically secure location?

Answer:
No. The CJI is encrypted in accordance with the CJIS Security Policy at rest. Therefore, only authorized users have access to the data. So, it is not required the server room be established as a physically secure location.

PERSONNEL ACCESS & SECURITY REQUIREMENTS

Scenarios

FAQ #2:

Question:
Our agency has a contract with a custodial service to provide cleaning services for our physically secure location. These personnel are all private contractors and have had fingerprint-based background checks to allow for unescorted access. Is security awareness training required?

Answer:
Yes. They may come across CJI material lying around on desks, displayed on computer screens, overhear discussions, etc. This is physical access to CJI. So, they should receive the first tier of security awareness training (All Personnel).

PERSONNEL ACCESS & SECURITY REQUIREMENTS

Questions?

BREAK

Hot Topics for Noncriminal Justice Agencies

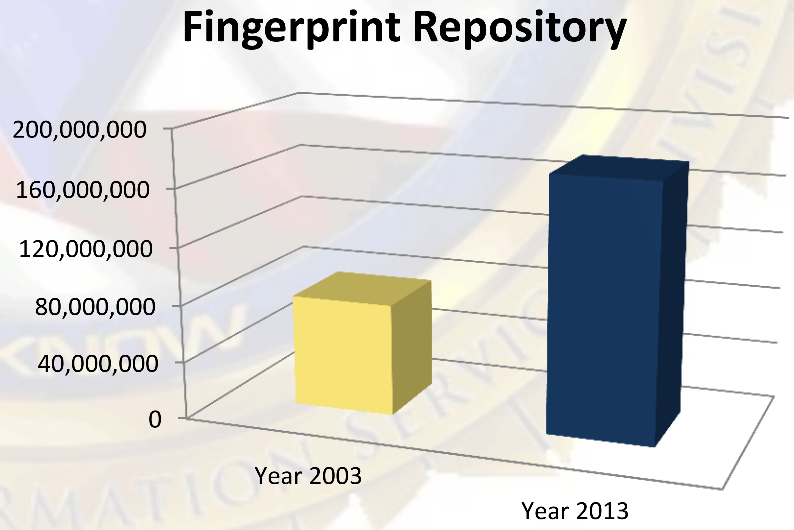
Lora Klingensmith

FBI CJIS ISO Sr. Management Program Analyst

Noncriminal Justice and the CJIS Security Policy

Repository:

- Since 1924, the FBI has been the national repository for fingerprints and related criminal history data. Over the years, the size of our fingerprint files has grown and the demand for the program's services has steadily increased.



Noncriminal Justice
and the CJIS Security Policy

Benefits:

- Safety & Trust
  - Of the 28 million civil submissions during 2013 approximately 2.5 million individuals identified as having existing criminal history records.

    - Protection of vulnerable populations

    - Trustworthy applicants

- Revenue
  - Monetary fees for processing civil fingerprint submissions offset the overhead and operational costs of the service, and for maintenance and technological refreshments to our national and state databases.

Noncriminal Justice
and the CJIS Security Policy

Processing:

- **Legislation** – why are you running the check?
  - Civil fingerprint checks are submitted to the FBI based upon a specific federal law authorizing a national fingerprint background check, or a state statute or municipal ordinance, if authorized by a state statute, authorizing a national background check in compliance with Public Law 92-544.

- **Technology** – how are you running the check and how are you receiving the response?
  - For its first 75 years of existence, the processing of incoming fingerprint cards by the FBI was predominantly a manual, time consuming, labor intensive process
  - On July 28, 1999 IAFIS changed the way we do business as it permitted the processing of all incoming fingerprint submissions in a totally electronic environment.
  - Livescan devices across the nation are now the predominant technology
  - CSP has had to conform to the technological advancements – efforts are continuous.

- **Distribution** - How are you sending responses to authorized recipient?
  - Mail (still) & web sites are predominant distribution

Noncriminal Justice
and the CJIS Security Policy

What is a Channeler?

- An FBI approved contractor, who has entered into an agreement with an Authorized Recipient(s), to receive noncriminal justice applicant fingerprint submissions and collect the associated fees.
- The Channeler ensures fingerprint submissions are properly and adequately completed, electronically forwards fingerprint submissions to the FBI's CJIS Division for national noncriminal justice criminal history record check, and receives electronic record check results for dissemination to Authorized Recipients.
- The Channeler is essentially an "expediter" rather than a user of criminal history record check results.
- Why is it important for you to know this?

Noncriminal Justice and the CJIS Security Policy

Security/Storage:

- Physically secure vs. Non-physically secure
  - When CHRI is stored, agencies shall establish appropriate administrative, technical and physical safeguards to ensure the security and confidentiality of the information.

Audit

- Officially begins October 1, 2014 for the NCJA community.

Training

- CJIS Security Policy – what relates to me?
  - Basic security awareness training shall be required within six months of initial assignment, and biennially thereafter, for all personnel who have access to CJI.

CJIS Security Policy
Appendix J

This appendix is not intended to be used in lieu of the CJIS Security policy but rather should be used as supplemental guidance.

Methodology:

Specifically for those NCJA with access to CJI as authorized by legislative enactment or federal executive order to request civil fingerprint-based background checks.

Who Benefits?

- For those NCJAs new to the CJIS security policy and APB auditing process (all NCJAs will be periodically audited by the CSA/SIB and may be included in a sampling of triennial audits conducted by the FBI*)* it is strongly recommended that each system processing CJI should be **individually** reviewed to determine which CSP requirements may apply.

HOT TOPICS FOR NONCRIMINAL JUSTICE AGENCIES

Questions?

NCJA Audit Update and Top Audit Findings

ITS Candice Preston

SITS Mike McIntyre

FBI CJIS Division Audit Unit

acjis@leo.gov

BACKGROUND

- IT Security Audit Overview
- Audit each CSA once every 3 years
- Review adherence to the CJIS Security Policy
- Scope has grown to include multiple CJIS Systems access
- October 2014 kicks off NCJA Audits

NCJA IT Security Audits

- Noncriminal Justice IT Security Audits
  - Kicking off October 1, 2014
  - 3 year zero-cycle audit
  - Will be auditing to all applicable CSP requirements
  - Corresponds to the CJA audit cycle
  - 3-4 NCJAs chosen within the state to start
  - Separate reports for NCJA and CJA

NCJA IT Security Audits

- Your Potential Challenges
  - Relatively new area to both auditors and audited
  - Limited resources
  - Different "languages" used
  - CSP/CJI may be a foreign concept to many NCJAs
  - Incorporating the Outsourcing Standard/Compact
- Our Challenges
  - Much the same!

NCJA IT Security Audits

- Where to begin?
  - Identifying/narrowing the scope of the audit
    - How are they getting the response (paper, livescan, website)?
    - What are they doing with the response (cabinet, local hard drive, RMS)?
    - Who, if anyone, are they sharing it with?
    - What are they doing to destroy it?

NCJA IT Security Audits

- Where to begin (continued)?
  - Mail-in Questionnaire
  - Narrow the scope to the access
    - Hard copy storage and accessibility
    - One user, one desktop storage and accessibility
    - Shared network storage and accessibility

NCJA IT Security Audits

- Where to begin (continued)?
  - The top outs that will follow this part of the presentation
  - Remember the CSP and audits are a continually improving process as was the journey from 4.5 to 5.3 today
    - "Zero cycle" from Sanctions
    - S&A Subcommittee yearly brief
    - Compact tailored brief?

NCJA IT Security Audits

Any questions before we move on to the next part of the presentation?

Question

- How many agencies did the IT Security Audit Program visit last year?

A. Less than 100

B. 196

C. 267

D. Over 300

Question

- How many agencies did the IT Security Audit Program visit last year?

A. Less than 100

B. 196

C. 267

D. Over 300

Question

- How many “shall” statements are in the *CJIS Security Policy*?

A. 136
B. 249
C. 368
D. Over 400

Question

- How many “shall” statements are in the *CJIS Security Policy*?

A. 136

B. 249

C. 368

D. Over 400

Background

- March 1, 2013 and February 28, 2014
  - 26 CJIS Systems Agencies (CSAs)
    - 21 States
    - 2 Repositories
    - 3 Federals
  - 229 Local Agencies

Background

What's being compared:

- 2013 = March 2013 through February 2014
- 2012 = March 2012 through February 2013
- 2011 = March 2011 through February 2012
- 2010 = March 2010 through February 2011

(previous cycle results for agencies audited in the past year)

Audit Findings

CSA Audit Findings Summary

March 2013 – February 2014

Audit Findings

March 2013 – February 2014

CSA Noncompliance Raw Data

Rank	Policy Area	Noncompliance Findings	Noncompliance Rate
1	Security Addendums	11	50%
2	Security Awareness Training	10	38%
3	Advanced Authentication	6	25%
3	Personnel Screening	6	23%
3	Authentication	6	23%
4	Security Audits	5	23%
4	Event Logging	5	19%
5	Encryption	4	15%
*	Management Control Agreements	3	25%

Percentages are determined by applicable policies at the 26 CSAs audited

Audit Findings

CSA Cycle Comparison

Rank	Policy Area	Noncompliance/Noncompliance Rate		
		2013	2012	2010
1	Security Addendums			
2	Security Awareness Training			
3	Advanced Authentication			
3	Personnel Screening			
3	Authentication			
4	Security Audits			
4	Event Logging			
5	Encryption			

Audit Findings
CSA Cycle Comparison

Rank	Policy Area	Noncompliance/Noncompliance Rate		
		2013	2012	2010
1	Security Addendums	11/50%		
2	Security Awareness Training	10/38%		
3	Advanced Authentication	6/25%		
3	Personnel Screening	6/23%		
3	Authentication	6/23%		
4	Security Audits	5/23%		
4	Event Logging	5/19%		
5	Encryption	4/15%		

Audit Findings

CSA Cycle Comparison

Rank	Policy Area	Noncompliance/Noncompliance Rate		
		2013	2012	2010
1	Security Addendums	11/50%		6/33%
2	Security Awareness Training	10/38%		4/19%
3	Advanced Authentication	6/25%		3/25%
3	Personnel Screening	6/23%		1/5%
3	Authentication	6/23%		6/29%
4	Security Audits	5/23%		4/19%
4	Event Logging	5/19%		0/0%
5	Encryption	4/15%		3/14%

Audit Findings
CSA Cycle Comparison

Rank	Policy Area	Noncompliance/Noncompliance Rate		
		2013	2012	2010
1	Security Addendums	11/50%	6/30%	
2	Security Awareness Training	10/38%	3/14%	
3	Advanced Authentication	6/25%	3/16%	
3	Personnel Screening	6/23%	4/18%	
3	Authentication	6/23%	5/23%	
4	Security Audits	5/23%	4/18%	
4	Event Logging	5/19%	1/5%	
5	Encryption	4/15%	3/14%	

Audit Findings

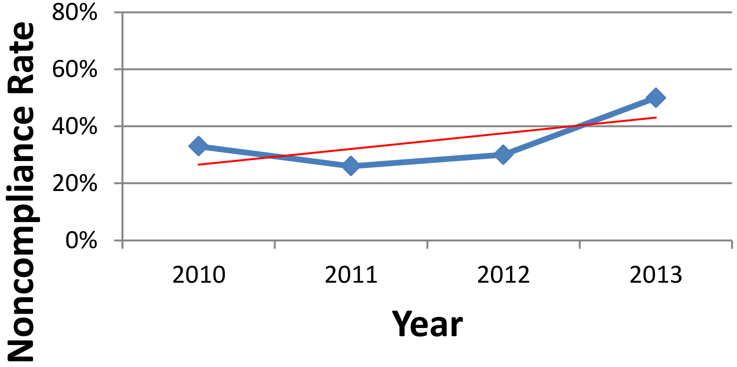
CSA Cycle Comparison

Rank	Policy Area	Noncompliance/Noncompliance Rate		
		2013	2012	2010
1	Security Addendums	11/50%	6/30%	6/33%
2	Security Awareness Training	10/38%	3/14%	4/19%
3	Advanced Authentication	6/25%	3/16%	3/25%
3	Personnel Screening	6/23%	4/18%	1/5%
3	Authentication	6/23%	5/23%	6/29%
4	Security Audits	5/23%	4/18%	4/19%
4	Event Logging	5/19%	1/5%	0/0%
5	Encryption	4/15%	3/14%	3/14%

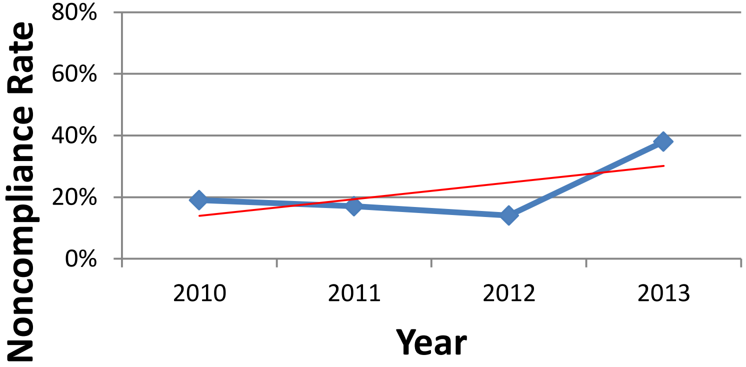
Audit Findings

Top CSA Audit Findings Trends

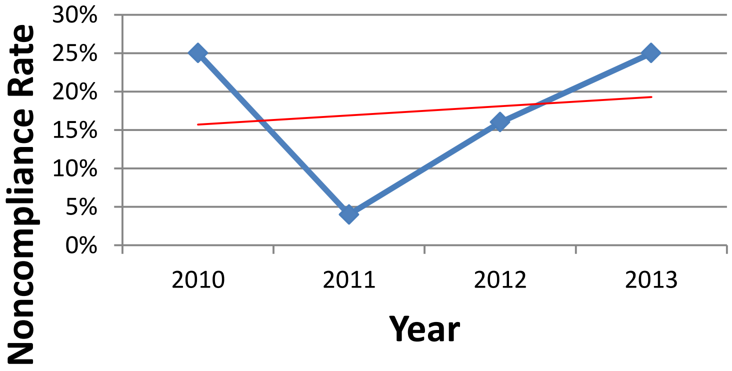
↑ Security Addendums



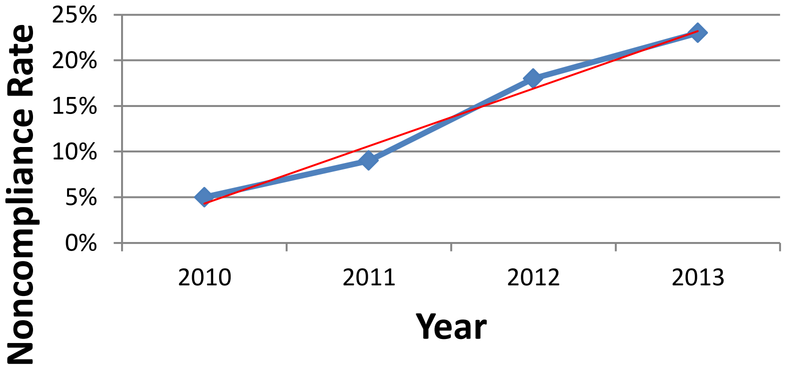
↑ Security Awareness Training



↑ Advanced Authentication



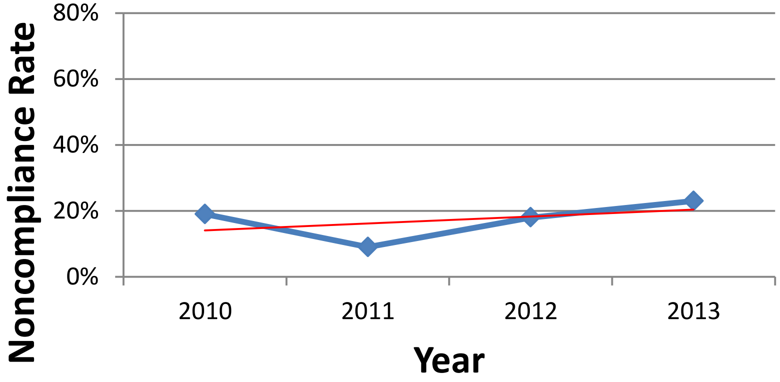
↑ Personnel Screening



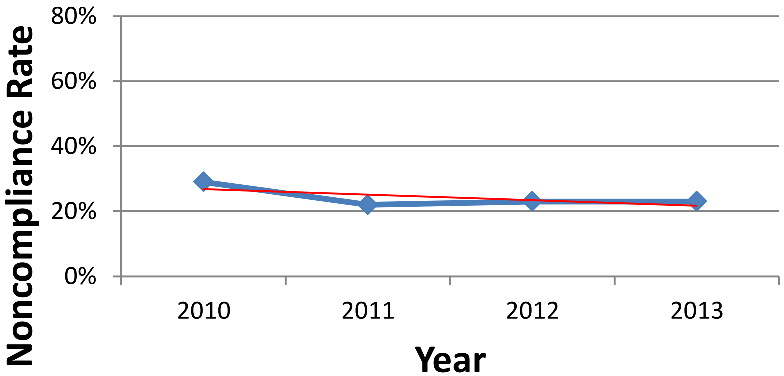
Audit Findings

Top CSA Audit Findings Trends

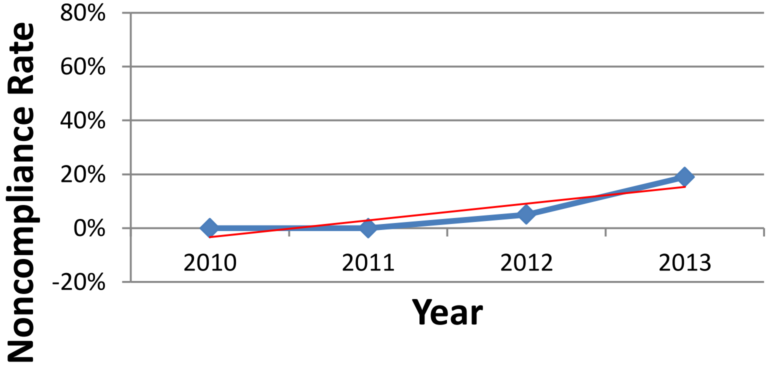
↑ Security Audits



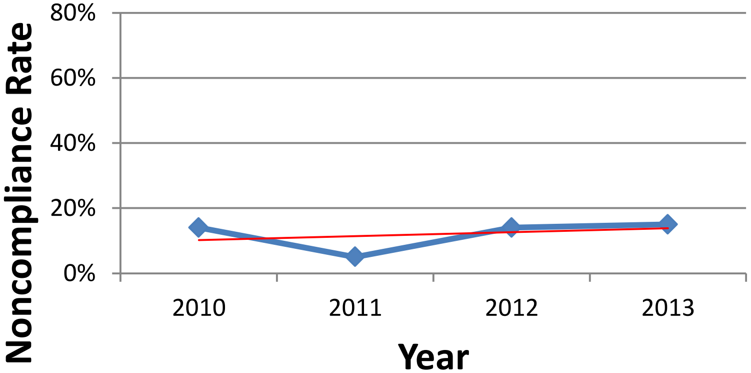
↓ Authentication



↑ Event Logging



↑ Encryption



Audit Findings

Local Audit Findings Summary

March 2013 – February 2014

Audit Findings

March 2013 – February 2014

Local Noncompliance Raw Data

Rank	Policy Area	Noncompliance Findings	Noncompliance Rate
1	Media Disposal	82	36%
2	Security Awareness Training	78	34%
3	Encryption	71	35%
4	Authentication	70	31%
5	Personnel Screening	67	29%
*	Security Addendums	54	43%
*	Management Control Agreements	49	33%

Percentages are determined out of applicable policies at the total 229 Local Agencies audited

Audit Findings
Local Cycle Comparison

Rank	Policy Area	Noncompliance/Noncompliance Rate		
		2013	2012	2010
1	Media Disposal			
2	Security Awareness Training			
3	Encryption			
4	Authentication			
5	Personnel Screening			
*	Security Addendums			
*	Management Control Agreements			

Audit Findings

Local Cycle Comparison

Rank	Policy Area	Noncompliance/Noncompliance Rate		
		2013	2012	2010
1	Media Disposal	82/36%		
2	Security Awareness Training	78/34%		
3	Encryption	71/35%		
4	Authentication	70/31%		
5	Personnel Screening	67/29%		
*	Security Addendums	54/43%		
*	Management Control Agreements	49/33%		

Audit Findings

Local Cycle Comparison

Rank	Policy Area	Noncompliance/Noncompliance Rate		
		2013	2012	2010
1	Media Disposal	82/36%		20/10%
2	Security Awareness Training	78/34%		59/30%
3	Encryption	71/35%		51/33%
4	Authentication	70/31%		69/37%
5	Personnel Screening	67/29%		44/22%
*	Security Addendums	54/43%		46/46%
*	Management Control Agreements	49/33%		43/36%

Audit Findings
Local Cycle Comparison

Rank	Policy Area	Noncompliance/Noncompliance Rate		
		2013	2012	2010
1	Media Disposal	82/36%	68/27%	
2	Security Awareness Training	78/34%	89/35%	
3	Encryption	71/35%	102/45%	
4	Authentication	70/31%	96/38%	
5	Personnel Screening	67/29%	86/34%	
*	Security Addendums	54/43%	115/60%	
*	Management Control Agreements	49/33%	75/63%	

Audit Findings

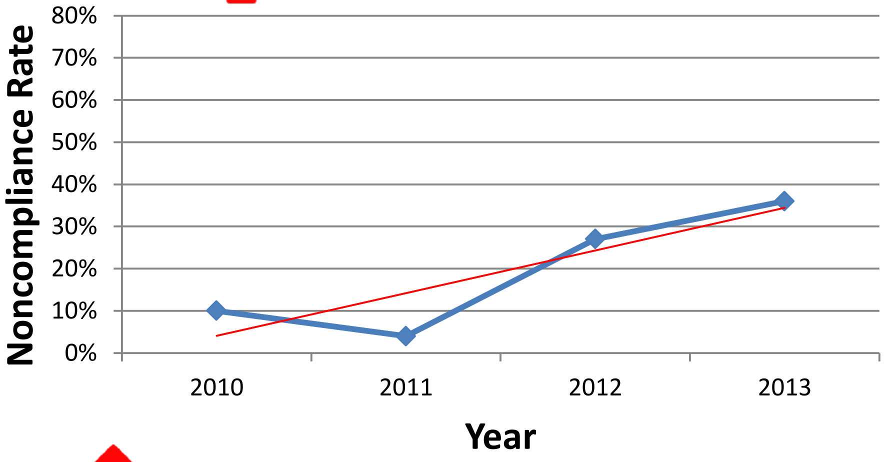
Local Cycle Comparison

Rank	Policy Area	Noncompliance/Noncompliance Rate		
		2013	2012	2010
1	Media Disposal	82/36%	68/27%	20/10%
2	Security Awareness Training	78/34%	89/35%	59/30%
3	Encryption	71/35%	102/45%	51/33%
4	Authentication	70/31%	96/38%	69/37%
5	Personnel Screening	67/29%	86/34%	44/22%
*	Security Addendums	54/43%	115/60%	46/46%
*	Management Control Agreements	49/33%	75/63%	43/36%

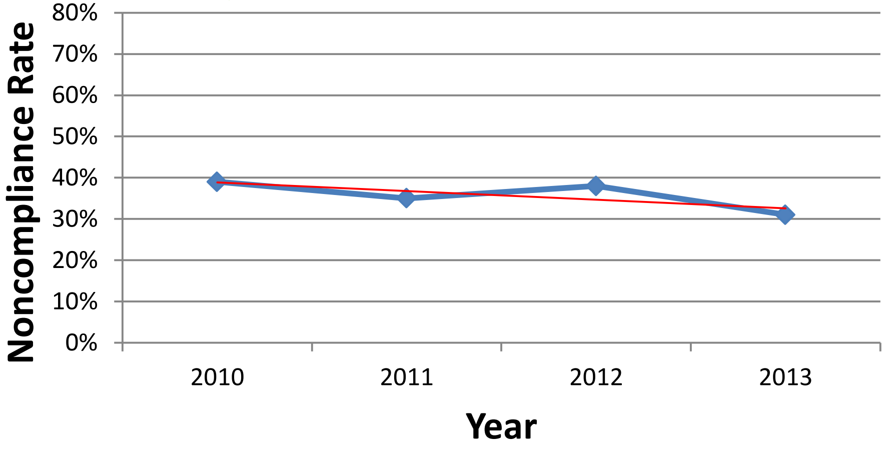
Audit Findings

Top Local Agency Audit Findings Trends

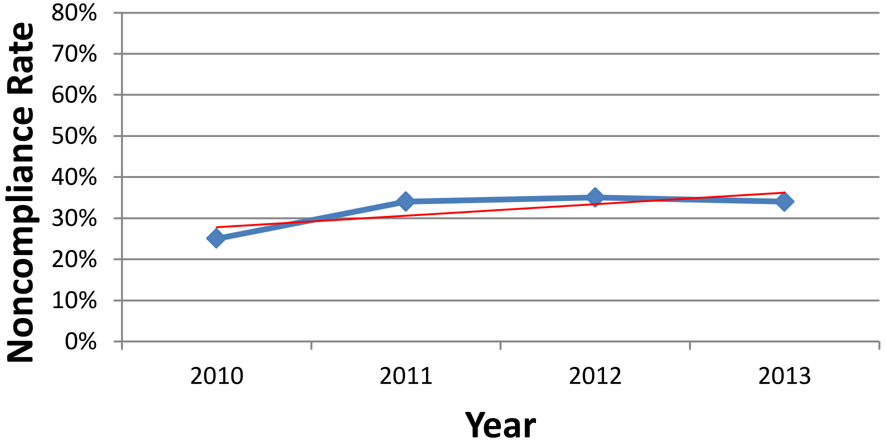
↑ Media Disposal



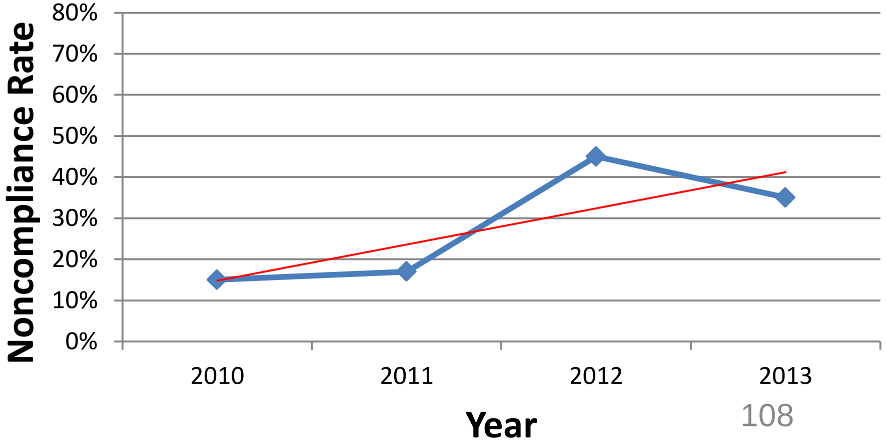
↓ Authentication



↑ Security Awareness Training

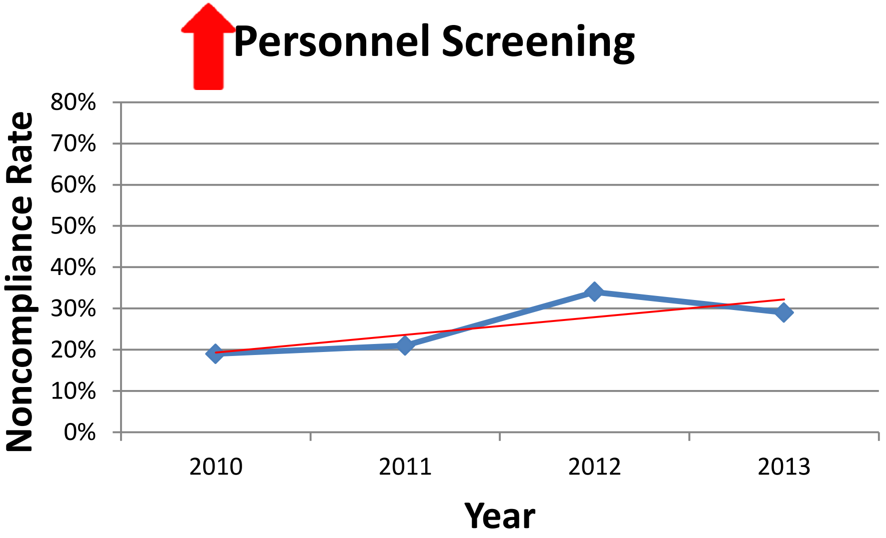


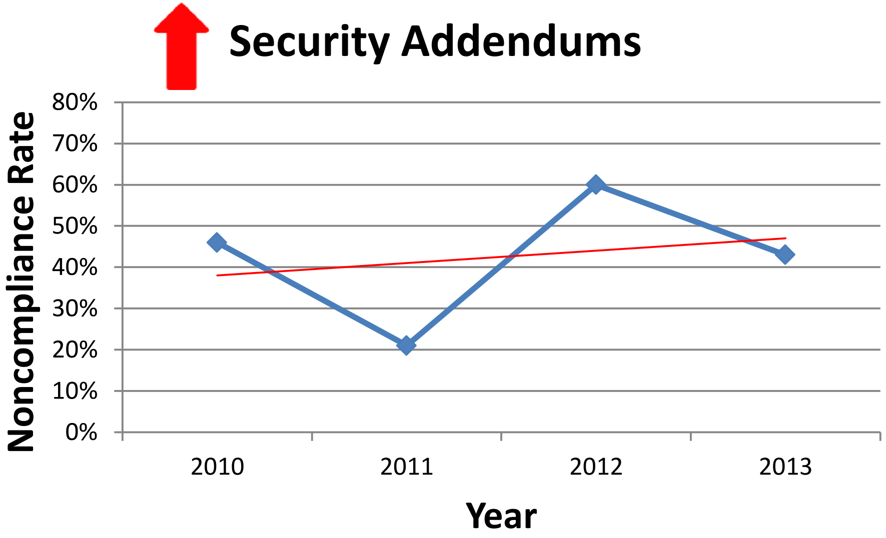
↑ Encryption

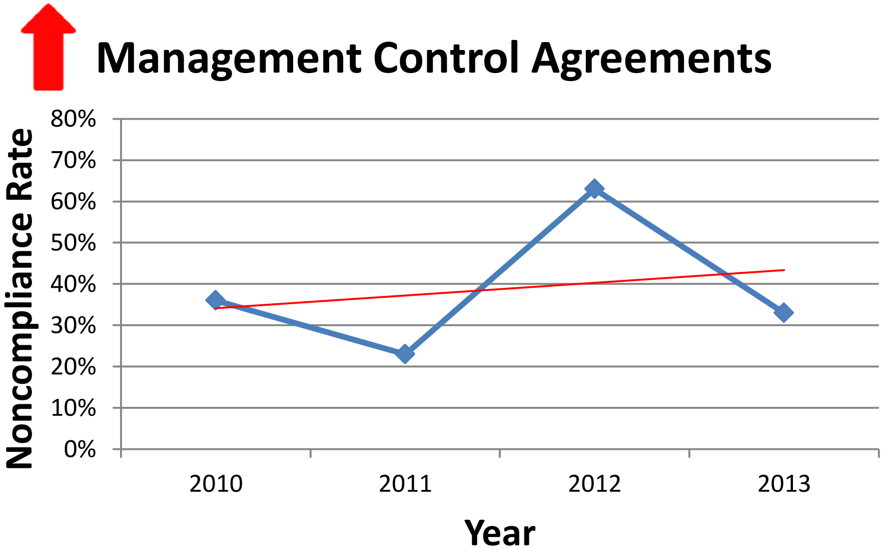


Audit Findings

Top Local Agency Audit Findings Trends







Repeat Offenders

So what are the top areas to keep an eye out for at the CSA and Local Agency level?

Repeat Offenders

CSA Top Findings	Local Agency Top Findings
Security Addendums	Media Disposal
Security Awareness Training	Security Awareness Training
Advanced Authentication	Encryption
Personnel Screening	Authentication
Authentication	Personnel Screening
Security Audits	Security Addendums
Event Logging	Management Control Agreements
Encryption	
Management Control Agreements	

Repeat Offenders

CSA Top Findings	Local Agency Top Findings
Security Addendums	Media Disposal
Security Awareness Training	Security Awareness Training
Advanced Authentication	Encryption
Personnel Screening	Authentication
Authentication	Personnel Screening
Security Audits	Security Addendums
Event Logging	Management Control Agreements
Encryption	
Management Control Agreements	

Repeat Offenders

Top Findings at Both CSA and Local Levels
Security Addendums
Security Awareness Training
Personnel Screening
Authentication
Event Logging
Encryption
Management Control Agreements

Audit Findings

CSA Audit New Policy Findings Summary

March 2013 – February 2014

Audit Findings
March 2013 – February 2014

CSA New Policy Noncompliance Raw Data

Rank	Policy Area	Noncompliance Findings	Noncompliance Rate
1	Identification/User ID (Acct. Validation)	10	38%
2	Media Protection (Written Policies)	7	27%
3	Media Disposal (Paper Policies, Witnessed)	5	19%
4	Physical Security (Policies)	4	17%
5	Event Logging (File Level, Log Review)	3	12%
*	Remote Maintenance (Written Justification)	2	67%
*	Sec. Awareness Training (Levels, Tier 1)	2	33%
*	System Use Notification	2	33%

Percentages are determined by applicable policies at the 26 CSAs audited

Audit Findings

Local Audit New Policy Findings Summary

March 2013 – February 2014

Audit Findings

March 2013 – February 2014

Local New Policy Noncompliance Raw Data

Rank	Policy Area	Noncompliance Findings	Noncompliance Rate
1	Physical Security (Written Policies)	88	39%
2	Media Protection (Written Policies)	78	34%
3	Identification/User ID (Acct. Validation)	75	34%
4	Media Disposal (Paper Policies, Witnessed)	78	34%
5	Event Logging (File Level, Log Review)	75	34%
*	System Use Notification	19	44%
*	Personally Owned Info. Systems (Policies)	8	47%
*	Remote Maintenance (Written Justification)	4	24%

Percentages are determined out of applicable policies at the total 229 Local Agencies audited

New Policy
Repeat Offenders

So what are the top new policy areas to keep an eye out for at the CSA and Local Agency level?

Repeat Offenders

CSA Top Findings	Local Agency Top Findings
Identification/User ID	Physical Security
Media Protection	Media Protection
Media Disposal	Identification/User ID
Physical Security	Media Disposal
Event Logging	Event Logging
Remote Maintenance	System Use Notification
Sec. Awareness Training	Personally Owned Info. Systems
System Use Notification	Remote Maintenance

Repeat Offenders

CSA Top Findings	Local Agency Top Findings
Identification/User ID	Physical Security
Media Protection	Media Protection
Media Disposal	Identification/User ID
Physical Security	Media Disposal
Event Logging	Event Logging
Remote Maintenance	System Use Notification
Sec. Awareness Training	Personally Owned Info. Systems
System Use Notification	Remote Maintenance

Repeat Offenders

Top New Policy Findings at Both CSA and Local Levels
Identification/User ID
Media Protection
Media Disposal
Physical Security
Event Logging
Remote Maintenance
System Use Notification

Coming on the Horizon

- 2011 New Policies will begin to be "Sanctionable" beginning October 1, 2014
  - Example: Physical Security Policies, Patch Management, Media Protection Policies, etc.

NCJA IT Security Audits

Questions?

LUNCH

On Your Own

Mobile Security

Jeff Campbell

FBI CJIS Assistant Information Security Officer

MOBILE SECURITY

Mobile Requirements Evolution

Fall 2011 Security and Access Subcommittee

- *"…creation of a matrix that lists the technology juxtaposed against the requirement."*
- Essentially: Would each device meet the Policy requirements?

Spring 2012 Security and Access Subcommittee

- *"…develop policy language to move towards a BlackBerry Enterprise Server-like standard for mobile devices."*
- BES represents the ideal managed environment with both policy and technical controls

Mobile Requirements Evolution

Spring 2013 Mobile Security Task Force created

- Chaired by Larry Coffee, FL-ISO, Vice-chair Alan Ferretti, TX-ISO
- Members comprised of state and local agency mobile SMEs:

  Michelle Young, Kent County, MI
  Jae Lim, Hawaii Criminal Justice Data Center
  Chris DeSain, NY Public Safety
  David Painter, Houston, TX PD
  Tom Jenkins, Ocala, FL PD

- Review topics related to mobile device security and provide recommendations to the S&A Subcommittee

MOBILE SECURITY

Who’s Winning the Battle?

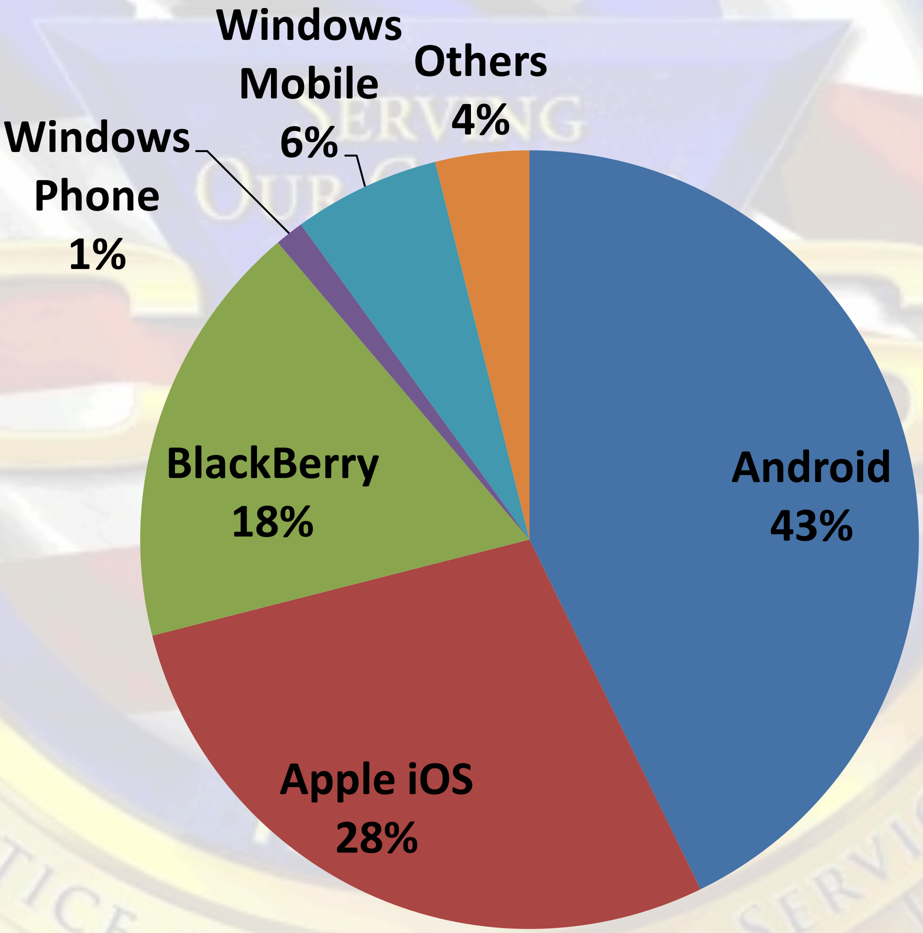
Operating

System

Device

Manufacturer

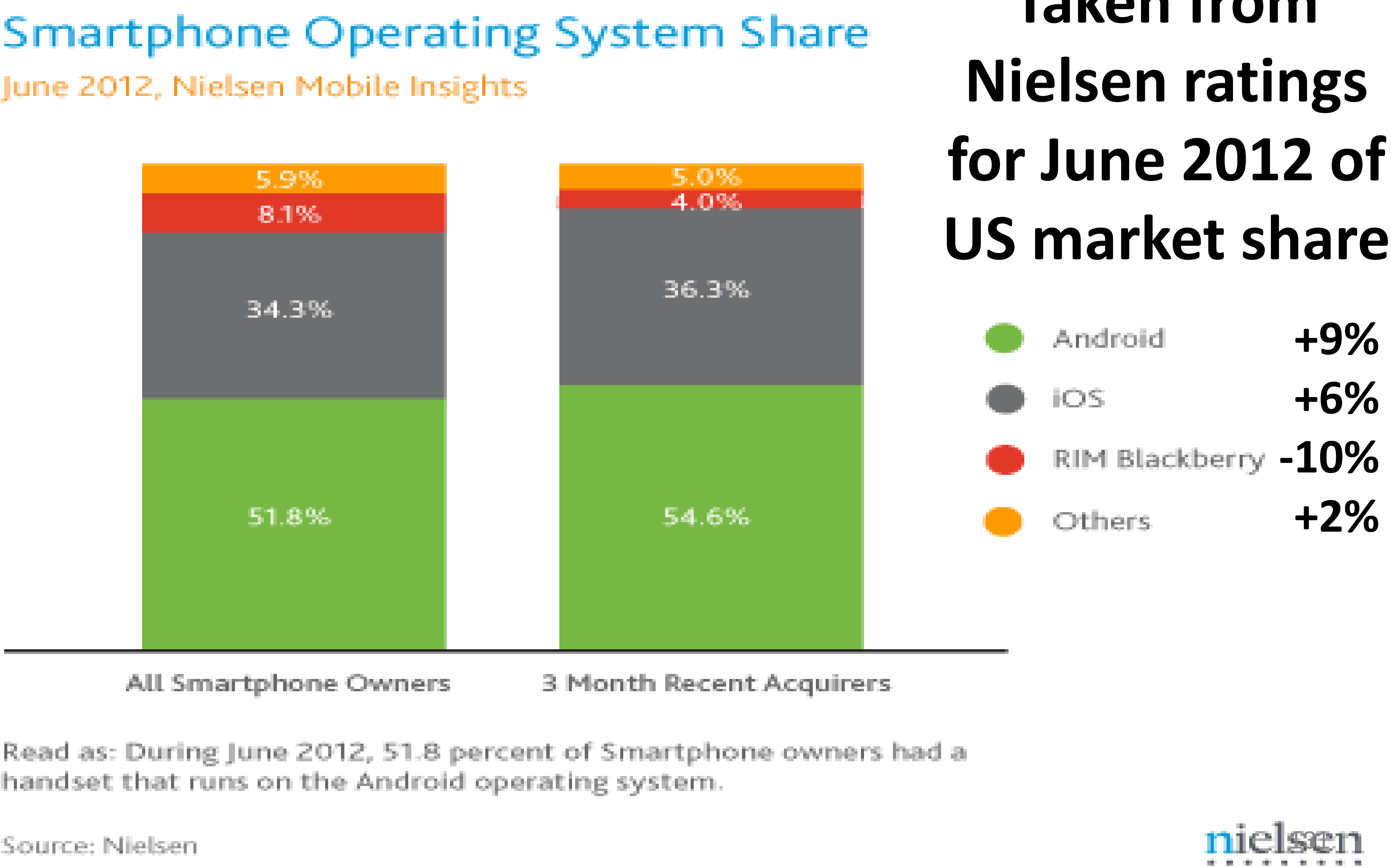
MOBILE SECURITY



Operating System Market Share

Taken from Nielsen ratings for Q3 2011 of US market share

MOBILE SECURITY



Smartphone Operating System Share

June 2012, Nielsen Mobile Insights

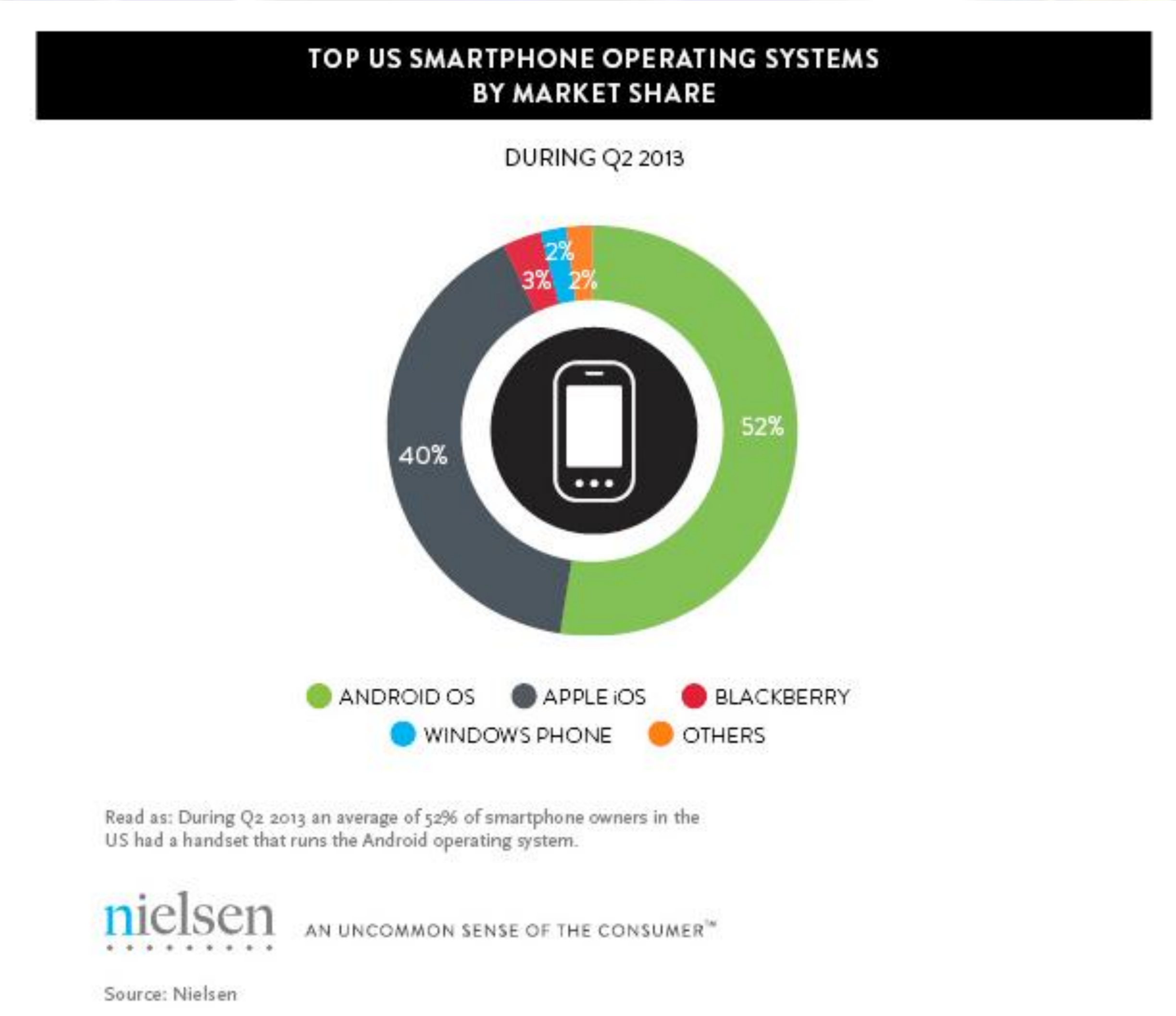
Read as: During June 2012, 51.8 percent of Smartphone owners had a handset that runs on the Android operating system.

Source: Nielsen

Taken from Nielsen ratings for June 2012 of US market share

🟢	Android	+9%
⚫	iOS	+6%
🔴	RIM Blackberry	-10%
🟠	Others	+2%

MOBILE SECURITY



TOP US SMARTPHONE OPERATING SYSTEMS
BY MARKET SHARE

DURING Q2 2013

Read as: During Q2 2013 an average of 52% of smartphone owners in the US had a handset that runs the Android operating system.

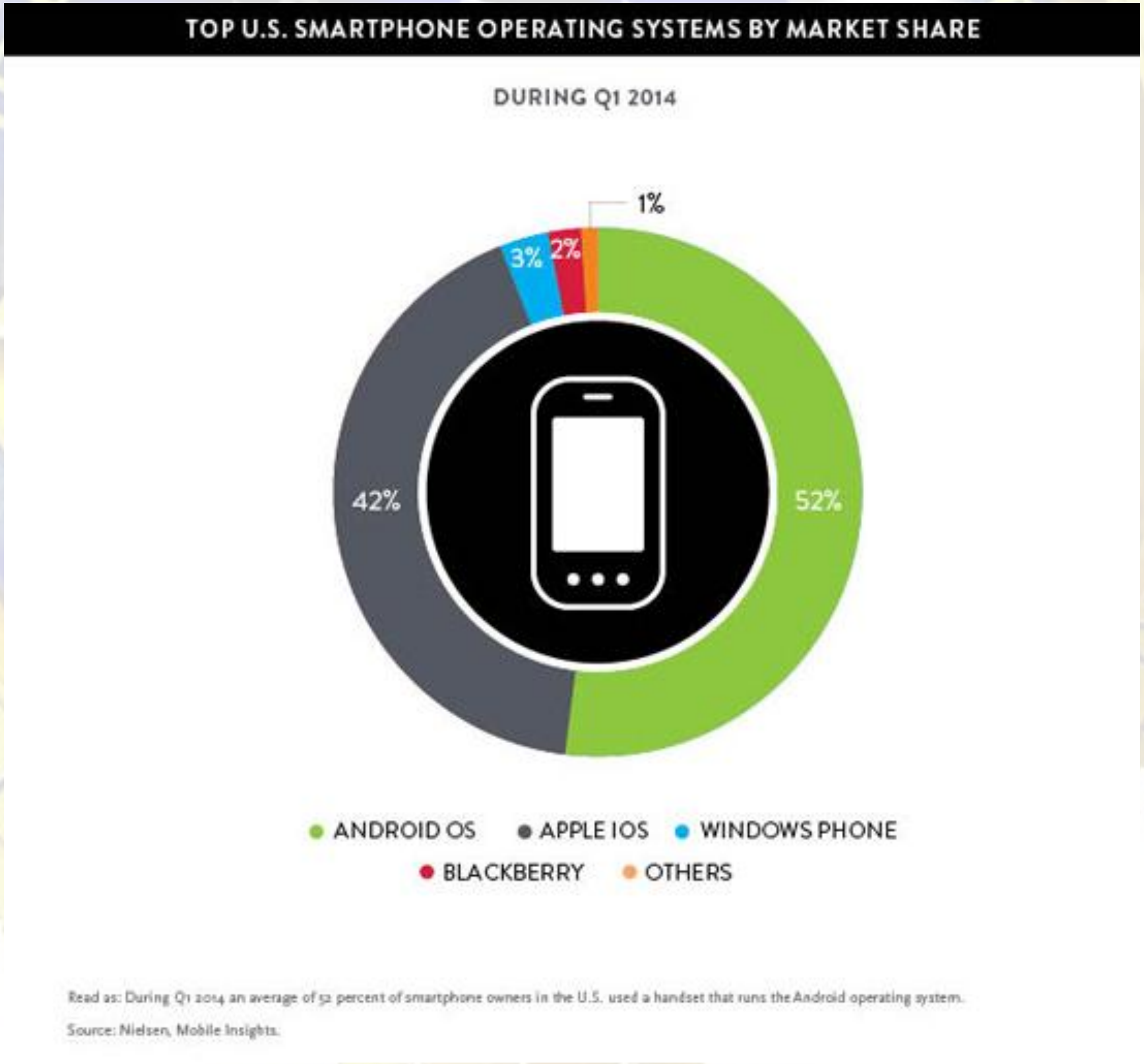
nielsen AN UNCOMMON SENSE OF THE CONSUMER™

Source: Nielsen

Nielsen U.S. Smartphone OS Market Share Q2 2013

Android NC
Apple iOS +6%
Blackberry -5%
Others -4%

MOBILE SECURITY



TOP U.S. SMARTPHONE OPERATING SYSTEMS BY MARKET SHARE

DURING Q1 2014

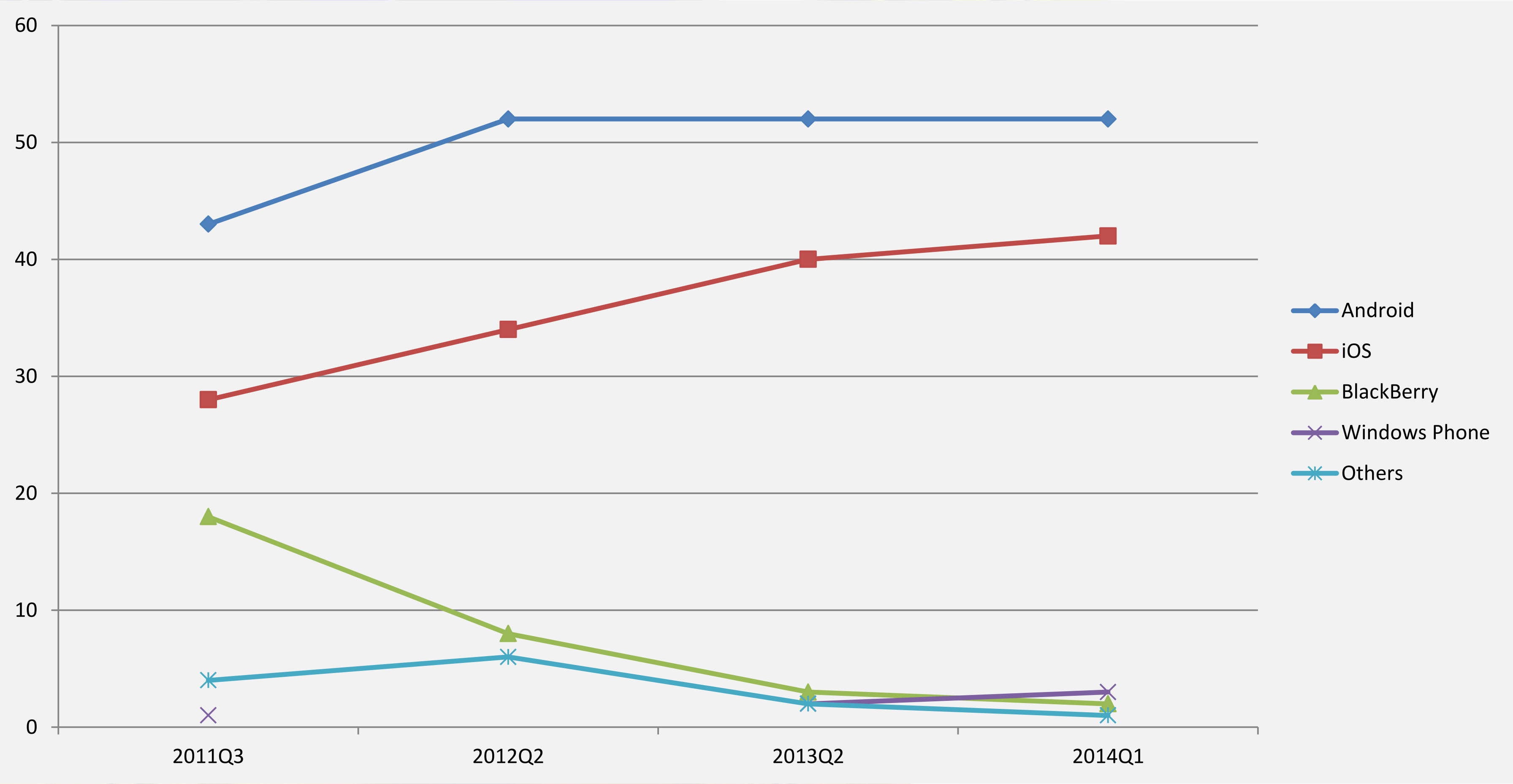
Read as: During Q1 2014 an average of 52 percent of smartphone owners in the U.S. used a handset that runs the Android operating system.

Source: Nielsen, Mobile Insights.

Nielsen U.S. Smartphone OS Market Share Q1 2014

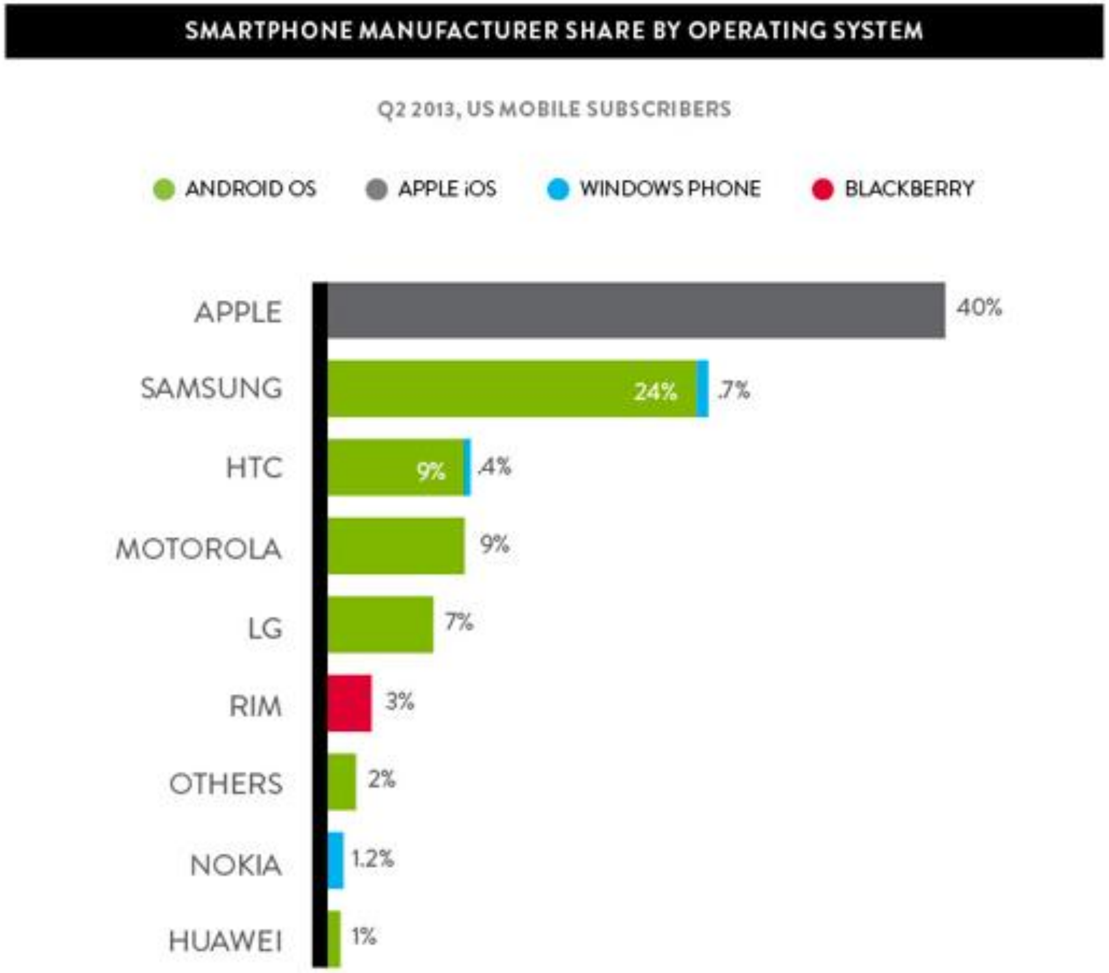
Android NC
Apple iOS +2%
Windows +1%
Blackberry -1%
Others -1%

MOBILE SECURITY



Trend of U.S. Smartphone OS Market

MOBILE SECURITY


SMARTPHONE MANUFACTURER SHARE BY OPERATING SYSTEM

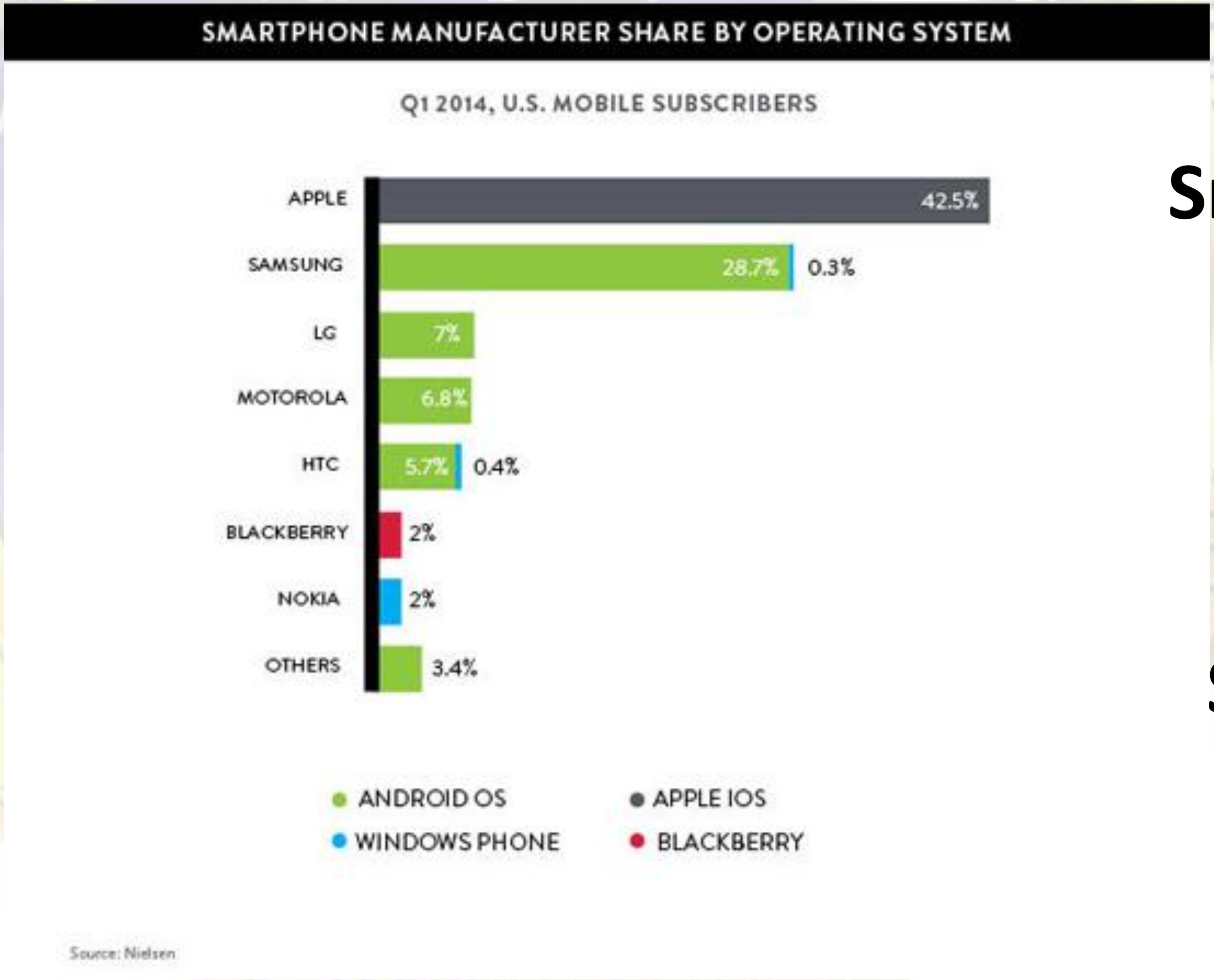
Q2 2013, US MOBILE SUBSCRIBERS

Read as: During Q2 2013, 24% of U.S. smartphone owners used Samsung's Android handsets and .7% had Samsung Windows Phone handsets

Source: Nielsen

Nielsen U.S. Smartphone OEM Market Share Q2 2013

MOBILE SECURITY



Source: Nielsen

Nielsen U.S. Smartphone OEM Market Share Q1 2014

Apple +2.5%
Samsung +4.3%
Blackberry -1%
HTC -3.3%

Mobile Devices: Where were we (5.2)?

Current mobile specific requirements:

- 5.5.6.1 – Personally Owned Information Systems
- 5.5.7 – Wireless Access Restrictions
- 5.5.7.3 – Cellular
- 5.5.7.3.1 – Cellular Risk Mitigations
- 5.5.7.3.2 – Voice Transmission Over Cellular Devices
- 5.5.7.3.3 – Mobile Device Management (MDM)
- 5.5.7.4 – Bluetooth

Mobile Devices: Where were we (5.2)?

Current generally applicable requirements:

- 5.3 – Incident Response
- 5.4 – Auditing and Accountability
- 5.5 – Access Control
- 5.10.4.2 – Malicious Code Protection
- 5.10.4.3 – Spam and Spyware Protection
- 5.10.4.4 – Personal Firewall

Mobile Devices: Where were we (5.2)?

5.5.7.3.1 Cellular Risk Mitigations

1. Apply available critical patches and upgrades to the operating system as soon as they become available for the device and after necessary testing as described in Section 5.10.4.1.
6. Employ personal firewalls or run a Mobile Device Management (MDM) system that facilitates the ability to provide firewall services from the agency level .
7. Employ antivirus software or run a MDM system that facilitates the ability to provide antivirus services from the agency level .

MOBILE SECURITY

Mobile Devices: Where were we (5.2)?

5.5.7.3.3 Mobile Device Management

- Centralized oversight of configuration control, application usage, and device protection and recovery [if so desired by the agency]
- No devices with unauthorized changes (rooted or jailbroken)
- Minimum MDM controls when allowing CJI access from

Mobile Devices: Where were we (5.2)?

5.5.7.3.3 Mobile Device Management

1. CJI is only transferred between CJI authorized applications and storage areas of the device.
2. MDM with centralized administration capable of at least:
   i. Remote locking of device
   ii. Remote wiping of device
   iii. Setting and locking device configuration
   iv. Detection of “rooted” and “jailbroken” devices
   v. Enforce folder or disk level encryption

Mobile Devices: Where are we now (5.3)?

A dedicated policy area (5.13)

- Consolidation of existing requirements
- Cross-reference to "general" requirements

Additional requirements based on the current G.4 Mobile Appendix

Mobile Device Categories

FORM FACTOR

Large Form Factor – vehicle mount or a carrying case and include a monitor with attached keyboard (MDTs/Laptops)

Medium Form Factor – vehicle mount or portfolio sized carry case that typically consist of a touch screen without attached keyboard (Tablets)

Small Form Factor –intended for carry in a pocket or ‘holster’ attached to the body (Smartphones)

Mobile Device Categories

Operating System (OS)

Full-feature OS – Windows, Linux/Unix, Apple OSX

Limited-feature OS – iOS, Android, BlackBerry

Mobile Device Categories

Three categories based on two characteristics

MDTs/Laptops

- Large form factor
- Full featured OS

Tablets

- Medium form factor
- Limited feature OS

Smartphones

- Small form factor
- Limited feature OS

Mobile Device Connectivity Types

Three (3) different types based on two (2) technologies

3G/4G Cell only – always on

WiFi only – could include cell “on demand”

3G/4G + Cell only (always on) *plus* WiFi “on demand”

Mobile Device Connectivity:

Cellular Only (Always On)

Cellular only connectivity characterized by:

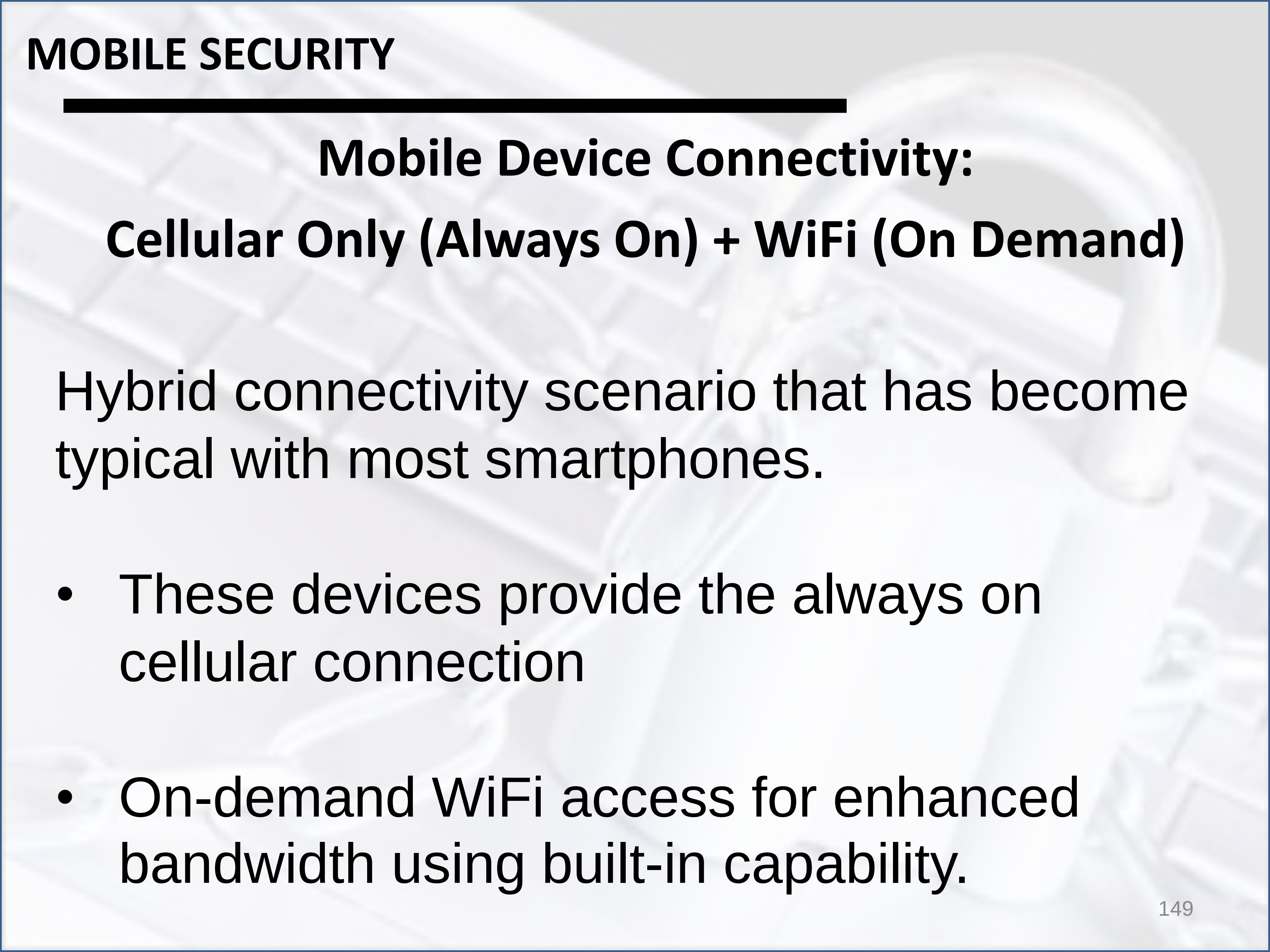
- ‘Always on’ network connection using the device internal radio to a network provider
- Reasonable assurance that device can be tracked, managed, or wiped remotely if lost or stolen

Mobile Device Connectivity:

WiFi Only (Cellular On-demand)

WiFi only connectivity is characterized by:

- Network access via a public or private hotspot or wireless access point
- Management and tracking not assured
- Could include cell on-demand



Mobile Device Connectivity:

Cellular Only (Always On) + WiFi (On Demand)

Hybrid connectivity scenario that has become typical with most smartphones.

- These devices provide the always on cellular connection

- On-demand WiFi access for enhanced bandwidth using built-in capability.

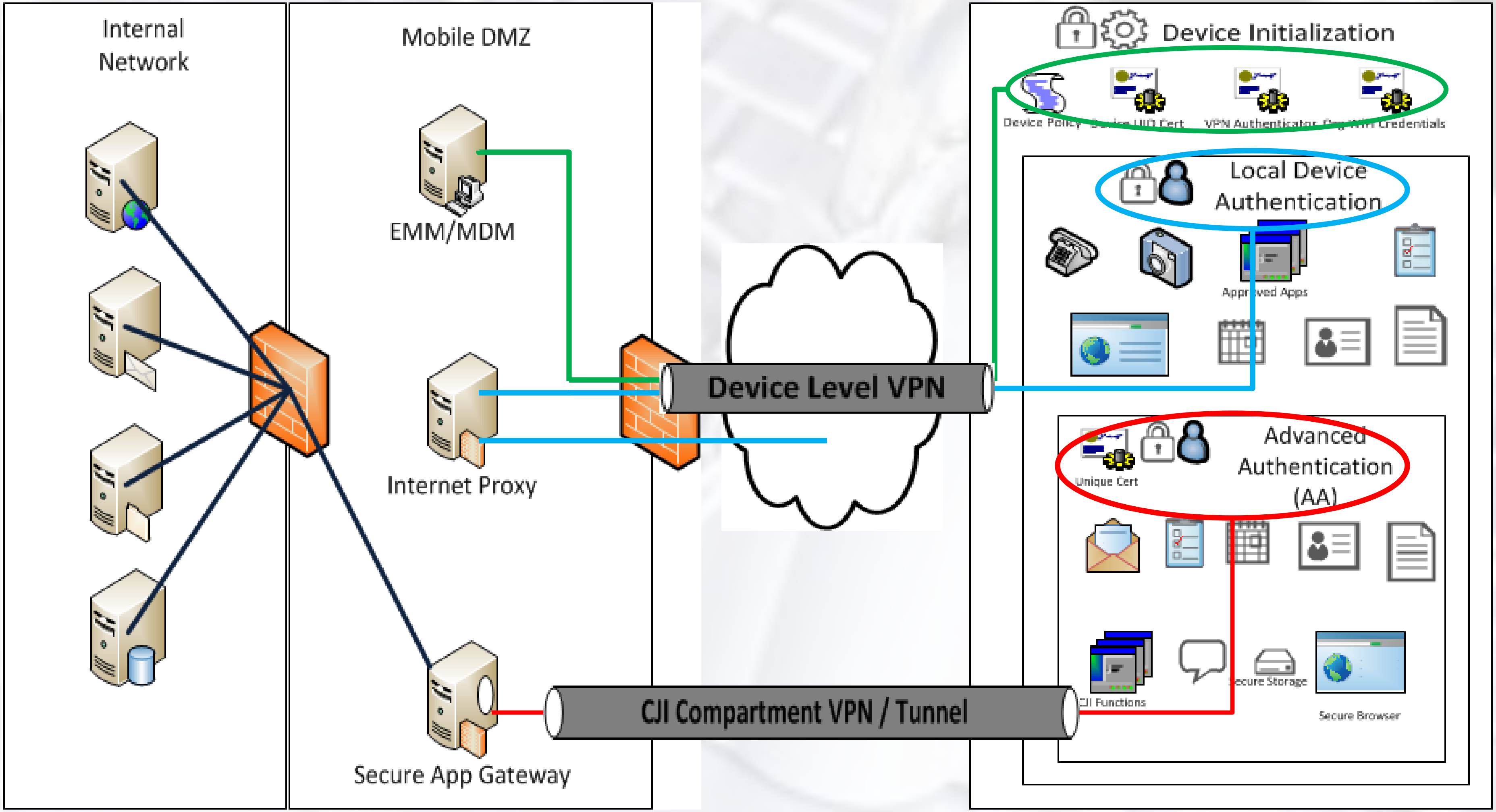
Mobile Device Connectivity Types

Three (3) different types based on two (2) technologies

		Device Categories		
		MDT / Laptops	Tablets	Pockets / Handhelds
Device Connectivity	cell only (always on)	X	X	√
	wifi only (includes 'on demand' cell)	√	√	X
	cell only (always on) + ‘on demand’ wifi	X	X	√

MOBILE SECURITY

Solution Example



Agency Network **Agency Issued Device**

Mobile Devices: Where are we now (5.3)?

5.13	New	Policy Area 13: Mobile Devices
5.13.1	5.5.7	Wireless Communication Technologies
5.13.1.1	5.5.7.1	All 802.11 Wireless Protocols
5.13.1.2	5.5.7.3	Cellular
5.13.1.3	5.5.7.4	Bluetooth
5.13.2	5.5.7.3.3	Mobile Device Management (MDM)
5.13.3	5.5.7.3.1	Wireless Device Risk Mitigations
5.13.4	New	System Integrity
5.13.4.1	New	Patching/Updates
5.13.4.2	New	Malicious Code Protection
5.13.4.3	New	Physical Protection
5.13.4.4	5.10.4.4	Personal Firewall
5.13.5	New	Incident Response
5.13.6	New	Auditing and Accountability
5.13.7	New	Access Control
5.13.8	New	Wireless Hotspot Capability
5.13.9	New	Identification and Authentication
5.13.9.1	New	Local Device Authentication
5.13.10	New	Device Certificates

MOBILE SECURITY

Mobile Devices: Where are we now (5.3)?

5.5.6.1 Personally Owned Information Systems

A personally owned information system shall not be authorized to access, process, store or transmit CJI unless the agency has established and documented the specific terms and conditions for personally owned information system usage. ~~*When bring your own devices (BYOD) are authorized, they shall be controlled using the requirements in Section 5.5.7.3 Cellular.*~~ ***When personally owned mobile devices (i.e. bring your own device [BYOD]) are authorized, they shall be controlled in accordance with the requirements in Policy Area 13: Mobile Devices.***

Mobile Devices: Where are we now (5.3)?

5.13.1 Wireless Communications Technologies

5.13.1.1 All 802.11 Wireless Protocols

Agencies shall ***implement the following controls for all agency managed wireless access points***:

5.13.1.2.2 Voice Transmissions Over Cellular Devices

Any cellular device used to transmit CJI via voice is exempt from the encryption and authentication requirements ~~when an officer determines there is an immediate need for the CJI to further an investigation or situations affecting the safety of an officer or the general public~~.

Mobile Devices: Where are we now (5.3)?

5.13.2 Mobile Device Management

1. CJI is only transferred between CJI authorized applications and storage areas of the device.
2. MDM with centralized administration capable of at least:
   i. Remote locking of device
   ii. Remote wiping of device
   iii. Setting and locking device configuration
   iv. Detection of “rooted” and “jailbroken” devices
   v. Enforce folder or disk level encryption
   vi. Application of mandatory policy settings on device
   vii. Detection of unauthorized configurations or software/applications

Mobile Devices: Where are we now (5.3)?

5.13.3 Wireless Device Risk Mitigations

5. Erase cached information, ***to include authenticators (see Section 5.6.2.1) in applications***, when session is terminated.
6. Employ personal firewalls or run a Mobile Device Management (MDM) system that facilitates the ability to provide firewall services from the agency level.
7. Employ antivirus software or run a MDM system that facilitates the ability to provide antivirus services from the agency level.

5.13.4.2 Malicious Code Protection

An appropriately configured MDM shall be used on smartphones and tablets to prevent the installation of unauthorized software or applications.

Mobile Devices: Where are we now (5.3)?

5.13.4.5 Personal Firewall

- "…employed on all mobile devices that ~~are mobile by design~~ ***have a full-featured operating system (i.e. laptops***~~, handhelds, personal digital assistants, etc.~~ ***or tablets with Windows or Linux/Unix operating systems).***"

- On limited-feature OS devices, application management using a MDM suffices.

Mobile Devices: Where are we now (5.3)?

5.13.5 Incident Response

- In addition to Section 5.3

- Additional reporting procedures in these situations:
  - Loss of device control (lock state, duration)
  - Total loss of device (CJI, lock state, remote wipe)
  - Device compromise
  - Device loss or compromise outside the U.S.

Mobile Devices: Where are we now (5.3)?

5.13.6 Auditing and Accountability

A mobile device not capable of providing required audit and accountability on its own accord shall be monitored by a MDM, other management system, or application capable of collecting required log data.

SANS SEC575: Mobile Device Security & Ethical Hacking Takeaways

- **MDM – must have, even rudimentary**
- **Application Management – malware/virus protection**
- **WiFi Considerations – just say no, unless absolutely required, cell service more secure**
- **Backend is Bigger Target – device not so much**
- **No Rooting/Jailbreaking – breaks inherent security features**

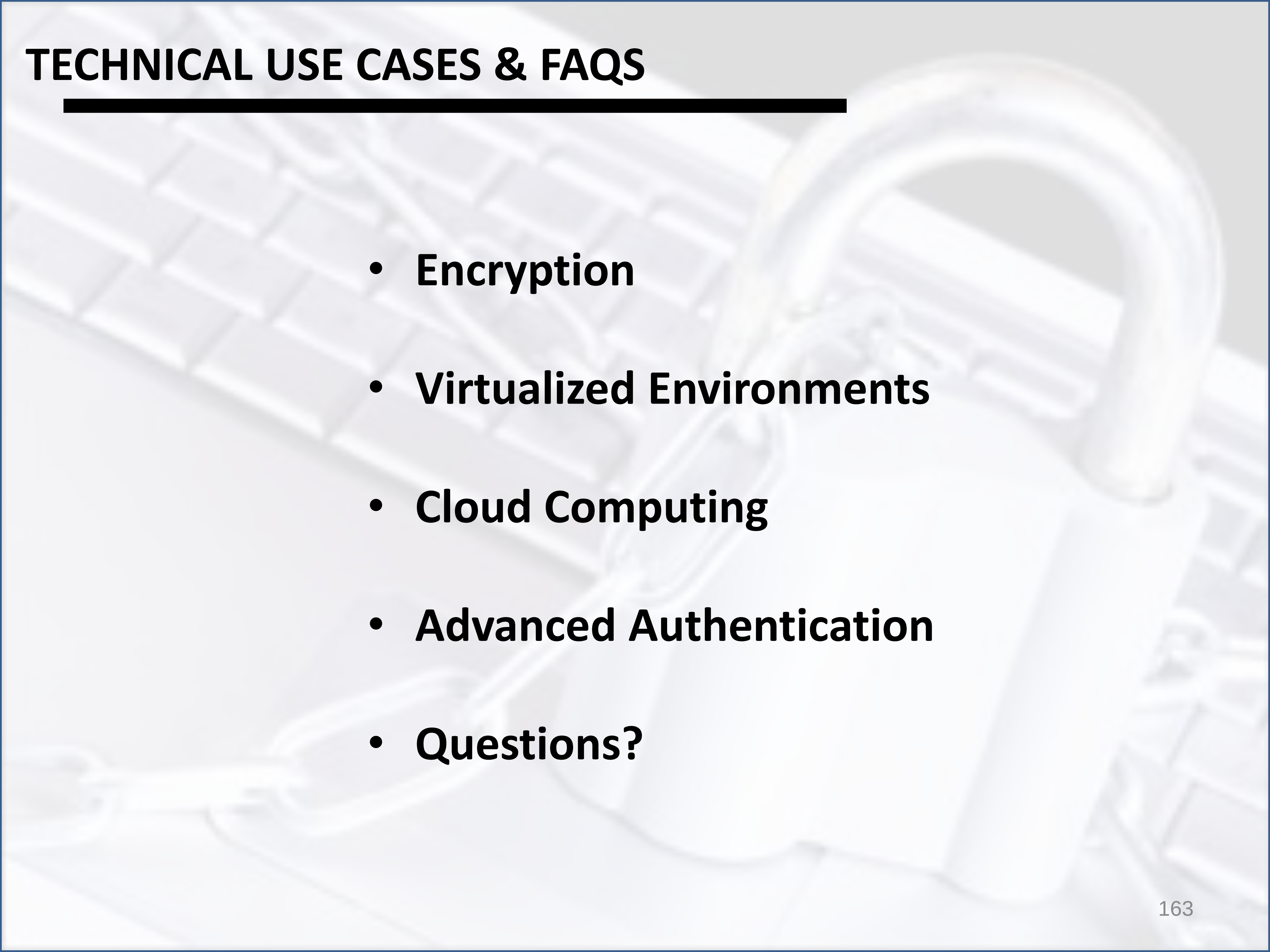
MOBILE SECURITY

Questions?

Technical Use Cases and FAQs

Steve Exley

FBI CJIS ISO Sr. Technical Analyst



TECHNICAL USE CASES & FAQS

- Encryption
- Virtualized Environments
- Cloud Computing
- Advanced Authentication
- Questions?

TECHNICAL USE CASES & FAQS

Encryption

TECHNICAL USE CASES & FAQS

Encryption

CJI must be encrypted when:

- Stored (at rest) outside the boundary of a physically secure location
- Immediately when transmitted outside the boundary of a physically secure location (two exceptions: 5.5.7.3.2 – cellular call and 5.10.2 - fax)
- When encryption is used for CJI:
  - ➢ In transit: must be FIPS 140-2 certified, at least 128 bit
  - ➢ At rest: can be FIPS 140-2 certified, 128 bit or AES, 256 bit

TECHNICAL USE CASES & FAQS

Encryption Use Case #1

Encryption for Data in Transit

- An officer has an agency-issued laptop used to remotely connect to the agency network.
- The officer establishes an encrypted (FIPS 140-2 certified, 128 bit) virtual private network (VPN) tunnel between his laptop and the agency.
- The agency requires the officer use Advanced Authentication (AA) at the network-VPN connection.
- The officer may run NCIC queries through this connection.

Note: Any CJI stored on the laptop would also be require protection via encryption.

Encryption Use Case #2

Encryption for Data at Rest

- A county board of education (BOE) is converting all employee records (may contain CJI) to electronic files.
- The files will be saved (stored, at rest) on a network server - server is NOT located in a secure data center.
- Therefore, the files are protected at rest via encryption (FIPS 140-2 certified, 128 bit **or** AES, 256 bit)
- The agency implemented the following access control measures:

  The agency is using folder encryption. Each folder contains different files. Each folder has its own CSP-compliant passphrase that provides access to all subsequent files within.

Encryption FAQ #1

Question:

If CJI is saved or stored on a laptop assigned to a police vehicle, must the CJI be encrypted?

Answer:

Per CJIS Security Policy v5.3, the police vehicle is a physically secure location. So, the applicable encryption requirements are the same as any other physically secure location: CJI may be saved unencrypted to a computer that is within a physically secure location, but if removed from the physically secure location (police vehicle) the encryption requirement comes into play.

TECHNICAL USE CASES & FAQS

Encryption FAQ #2

Question:

How Do I Check for FIPS 140-2 Certification?

Answer:

FIPS certification information can be found at the following NIST links:

- FIPS 140-2 Modules Currently in Testing:
  - ➢ http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140InProcess.pdf
- FIPS 140-2 Certifications Sorted by Vendor
  - ➢ http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/1401vend.htm
- All Certified FIPS 140-2 Cryptographic Modules
  - ➢ http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140val-all.htm

TECHNICAL USE CASES & FAQS

Virtualized Environments

TECHNICAL USE CASES & FAQS

Virtualized Environments

There are a few specific security control requirements that need to be implemented to mitigate inherent vulnerabilities, such as:

- Isolating the host from the virtual machine (VM)
- Maintaining audit logs for all VMs and hosts and store the logs outside the host's virtual environment.
- Separating/segregating Internet facing VMs (web servers, portal servers, etc.) from VMs that process CJI internally (current Policy states physical separation – working to change this).
- Ensuring "critical" device drivers are not shared

TECHNICAL USE CASES & FAQS

Virtualized Environments

The following are technical security industry best practices and should be implemented wherever feasible:

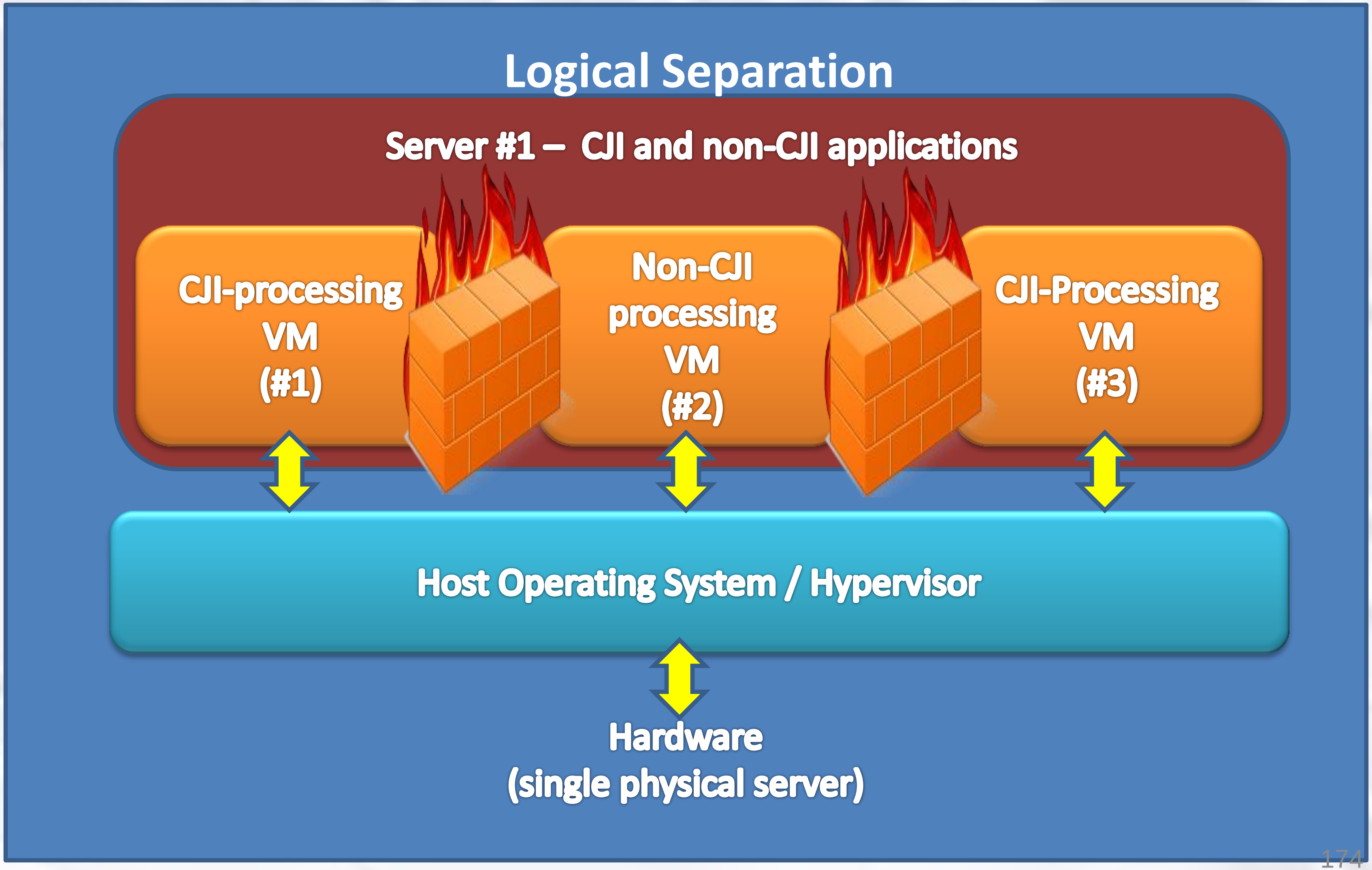
- Encrypt network traffic between the virtual machine and host.
- Implement IDS and IPS monitoring within the virtual machine environment.
- Virtually firewall each virtual machine from each other (or physically firewall each virtual machine from each other with an application layer firewall) and ensure that only allowed protocols will transact.
- Segregate the administrative duties for the host.

Virtualized Environments Use Case #1

Logical Separation

- A PD network was incorporated within a virtualized network as part of a county network consolidation effort.
- The virtual network consists of both CJI and non-CJI processing virtual machines (VM).
- So, the VMs are segregated (CJI-processing VMs from non-CJI VMs) and separated via virtual firewalls.
- The agency has adapted the industry best practice recommendation of encrypting network traffic between the VM and the Host.
- The virtual network resides completely within a physically secure location (no remote connections), so encryption is not a requirement for CJI at rest.

Virtualized Environments



Logical Separation
Server #1 – CJI and non-CJI applications
CJI-processing VM (#1)
Non-CJI processing VM (#2)
CJI-Processing VM (#3)
Host Operating System / Hypervisor
Hardware (single physical server)

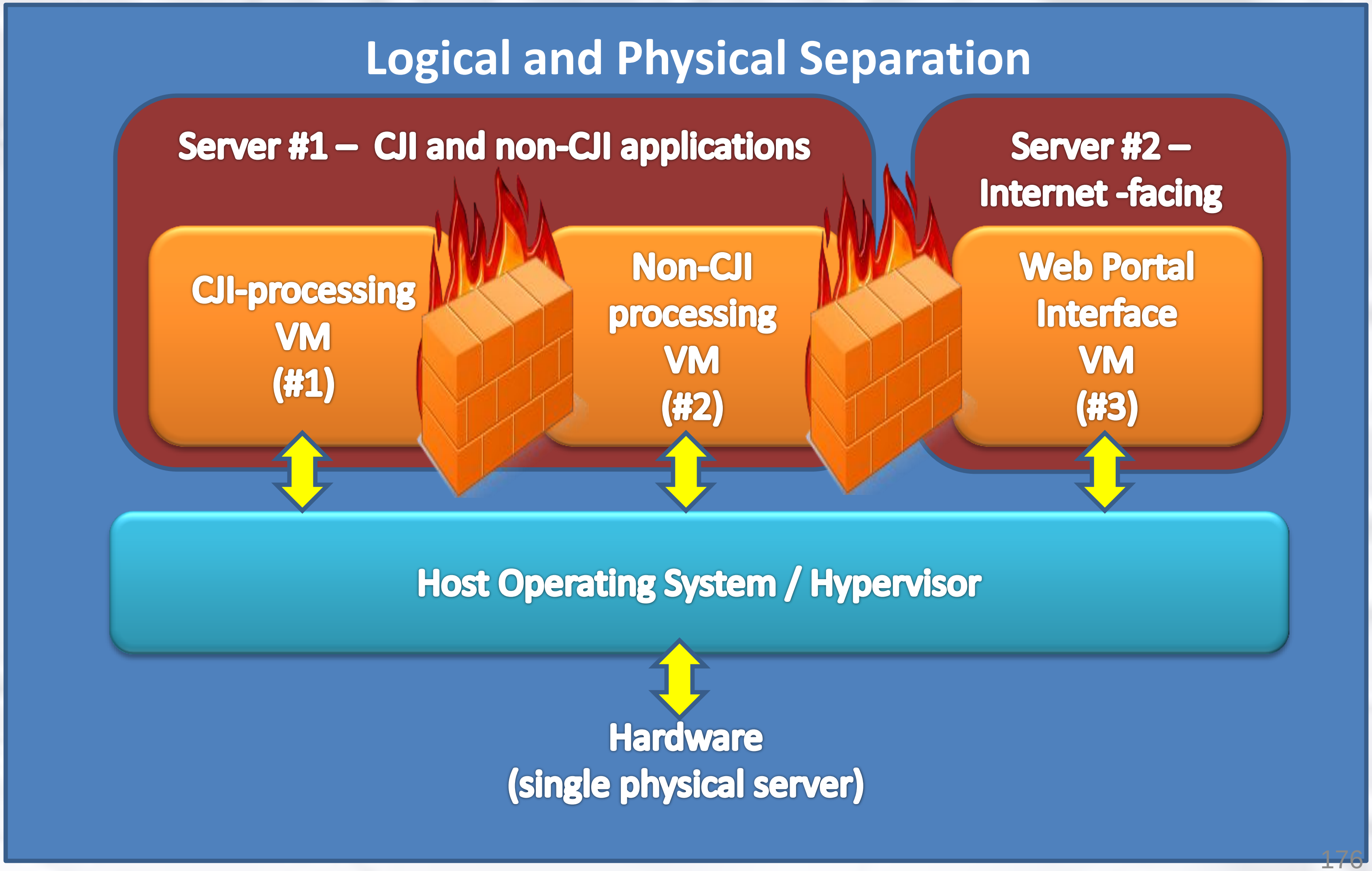
Virtualized Environments Use Case #1

Physical and Logical Separation

- The state police (SP) recently transitioned to a virtualized network.
- The entire network resides completely within the PD which is a physically secure location – no encryption requirement for CJI at rest.
- The SP manages the state switch and will allow remote connections to from the virtual network via a web portal interface – link is protected via encryption (FIPS 140-2 certified, 128 bit)
- Internet facing VM (web portal interface) is physically separated from non-Internet facing VMs.
- The network consists of both CJI and non-CJI processing virtual machines (VM) - VMs are segregated (CJI-processing VMs from non-CJI VMs) and separated via virtual firewalls.

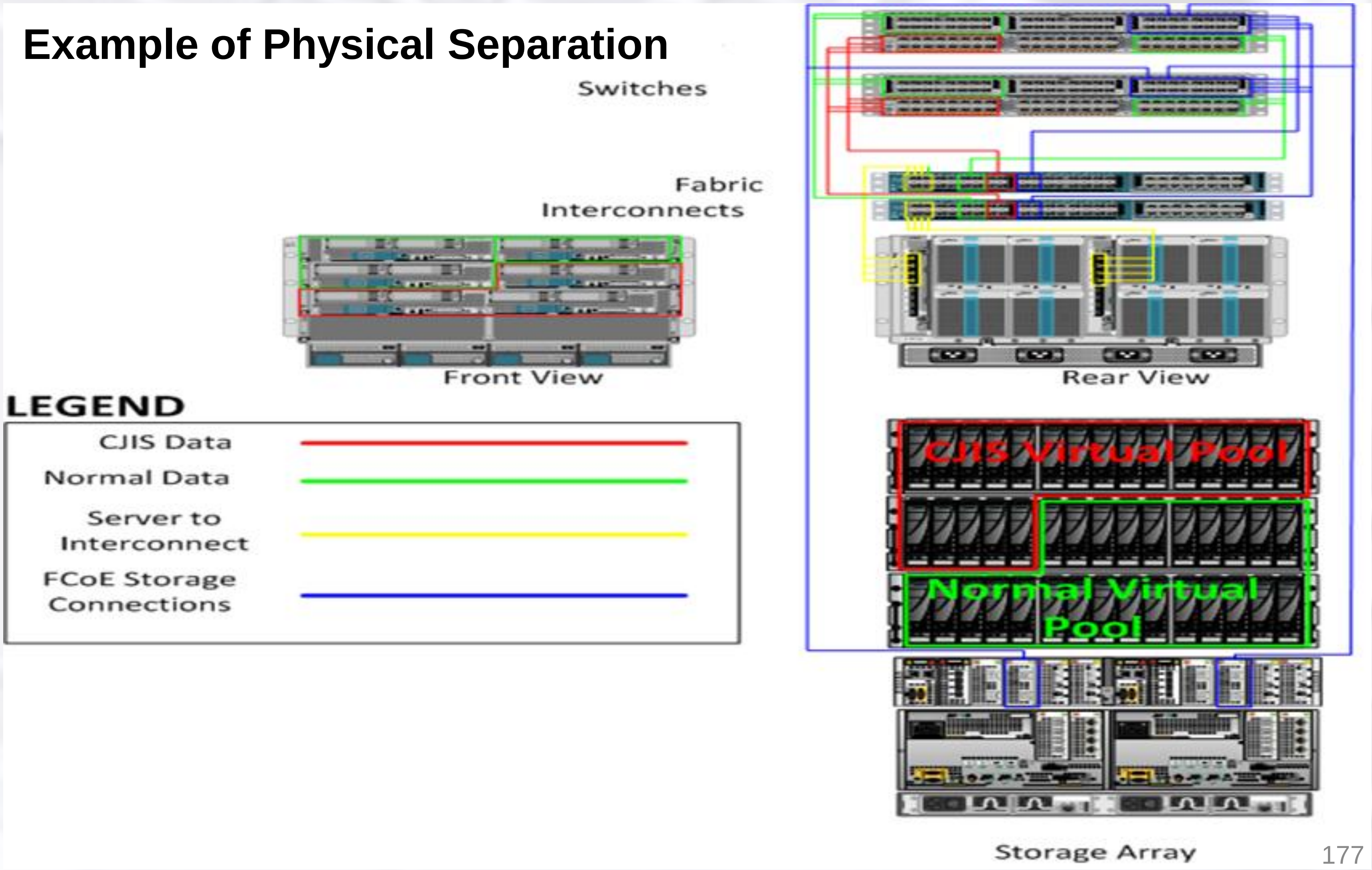
TECHNICAL USE CASES & FAQS

Virtualized Environments


Logical and Physical Separation
Server #1 – CJI and non-CJI applications
Server #2 – Internet -facing
CJI-processing VM (#1)
Non-CJI processing VM (#2)
Web Portal Interface VM (#3)
Host Operating System / Hypervisor
Hardware (single physical server)

Virtualized Environments

Example of Physical Separation



Virtualized Environments FAQ #1

Question:
In section 5.10.3.2 Virtualization, item number 3 in the second paragraph states:

"Virtually firewall each virtual machine from each other (or physically firewall each virtual machine from each other with an application layer firewall) and ensure that only allowed protocols will transact."

So, is this a requirement? Will this be audited?

Answer:
No. This is not an auditable requirement. It is simply industry best practice guidance. Appendix G.1 provides some additional best practice guidance to provide better security for your virtualized environment.

Virtualized Environments FAQ #2

Question:

In section 5.10.3.2 Virtualization, Item number 4 states:

"Device drivers that are “critical” shall be contained within a separate guest."

I am not sure what this requirement is asking? Does this mean that critical device drivers should be stored in separate virtual machine?

Answer:

The requirement is to place the critical drivers for each guest (or more specifically, VM) within that guest/VM. In other words, don’t store the drivers in the hypervisor, or host operating system, for sharing. The intent is for each VM to be treated as their own systems – secured independently.

TECHNICAL USE CASES & FAQS

Cloud Computing

Cloud Computing

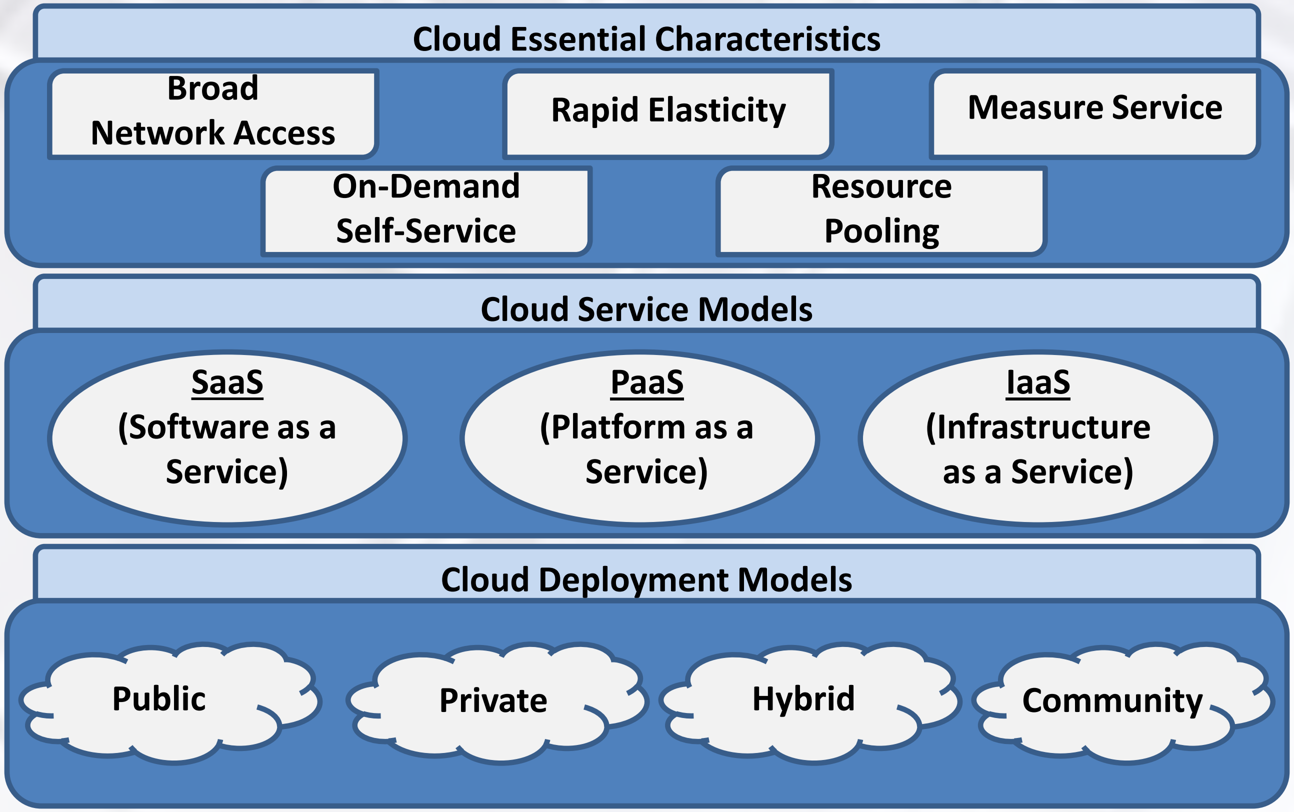
What is Cloud Computing?

- Defined by the CJIS Security Policy as:

  A distributed computing model that permits on-demand network access to a shared pool of configurable computing resources (i.e., networks, servers, storage, applications, and services), software, and information.

Cloud Computing

The Cloud Model Explained



Cloud Essential Characteristics

Broad Network Access

Rapid Elasticity

Measure Service

On-Demand Self-Service

Resource Pooling

Cloud Service Models

SaaS (Software as a Service)

PaaS (Platform as a Service)

IaaS (Infrastructure as a Service)

Cloud Deployment Models

Public

Private

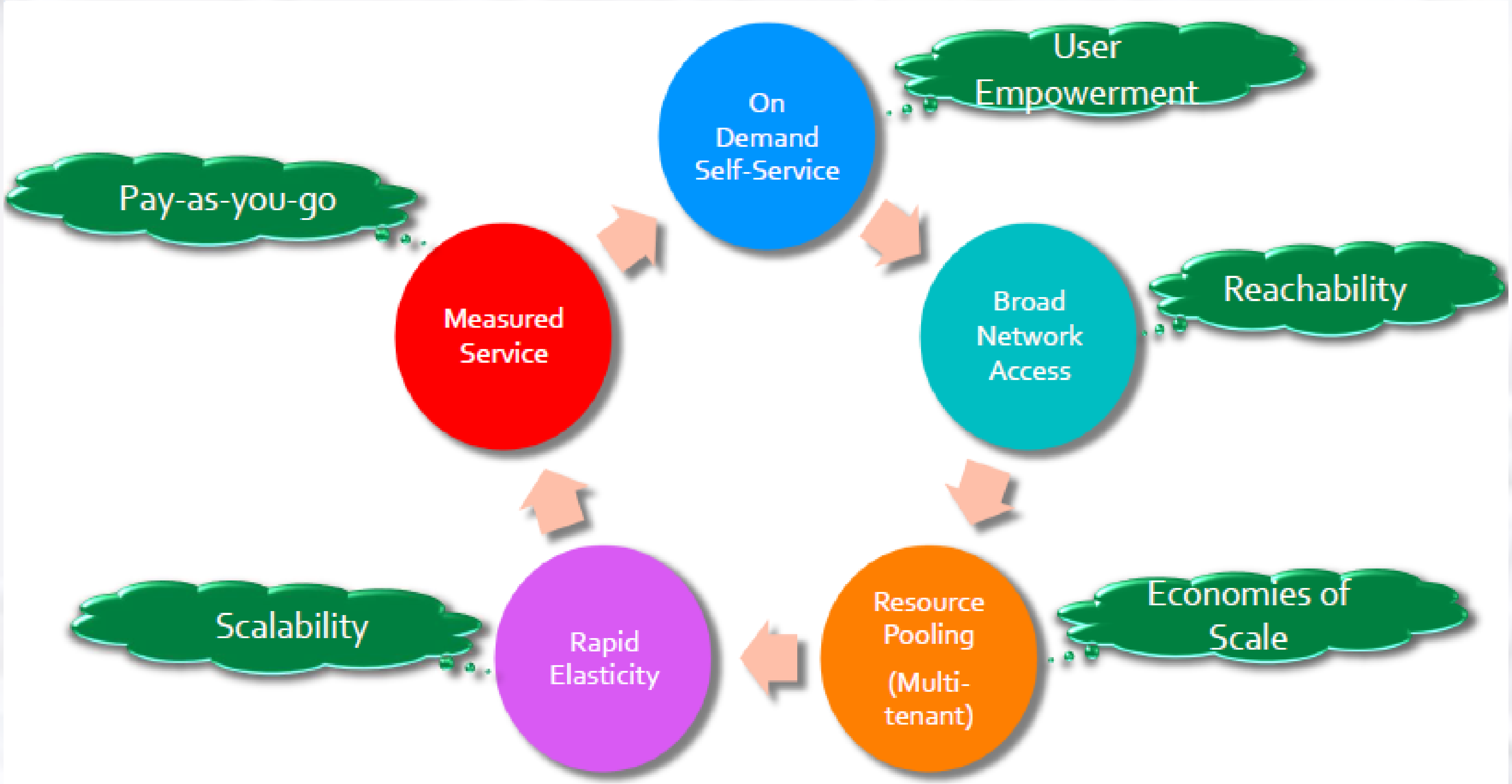
Hybrid

Community

TECHNICAL USE CASES & FAQS

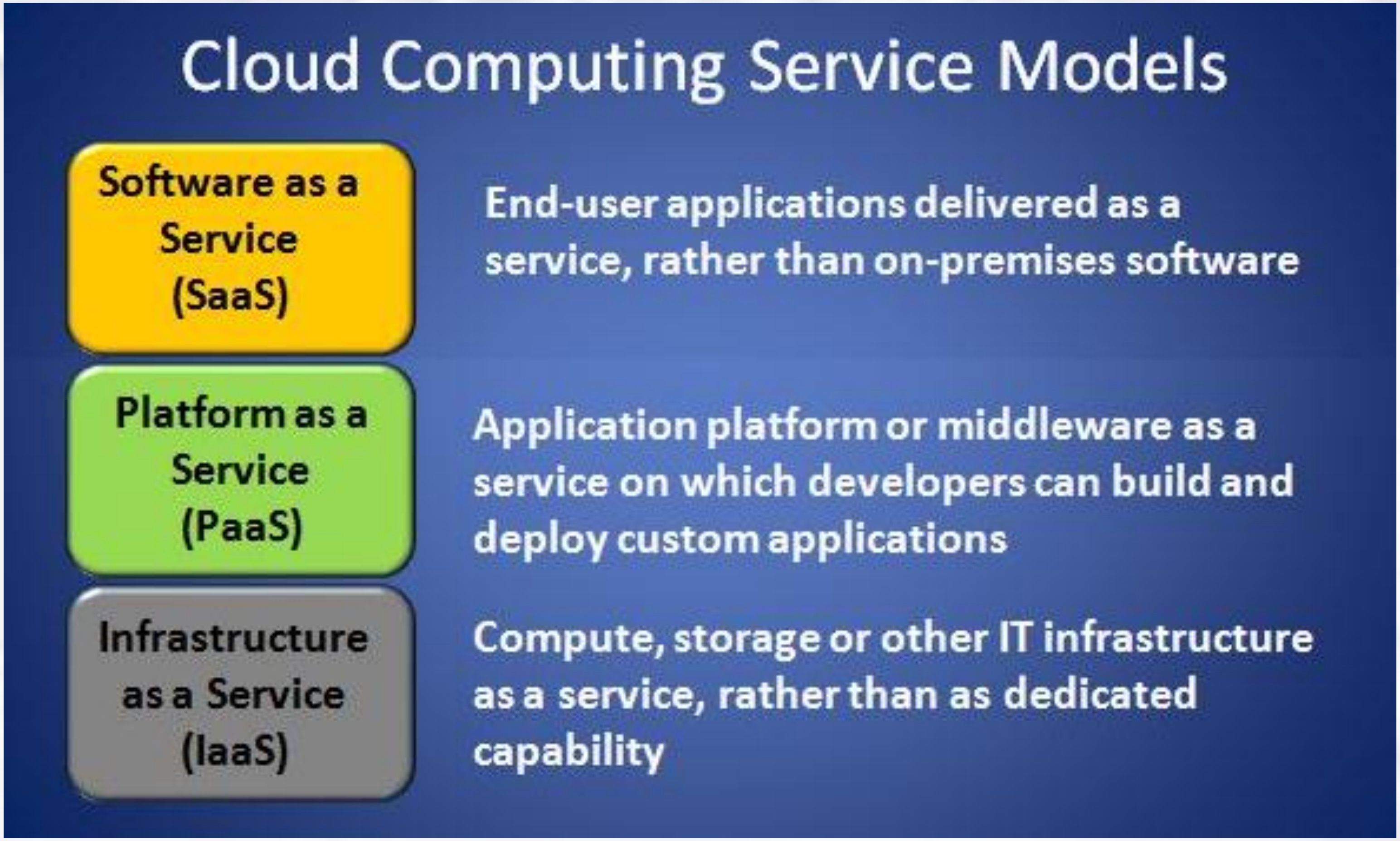
Cloud Computing

Cloud Essential Characteristics



Cloud Computing

Cloud Service Models



Cloud Computing Service Models

Software as a Service (SaaS)

End-user applications delivered as a service, rather than on-premises software

Platform as a Service (PaaS)

Application platform or middleware as a service on which developers can build and deploy custom applications

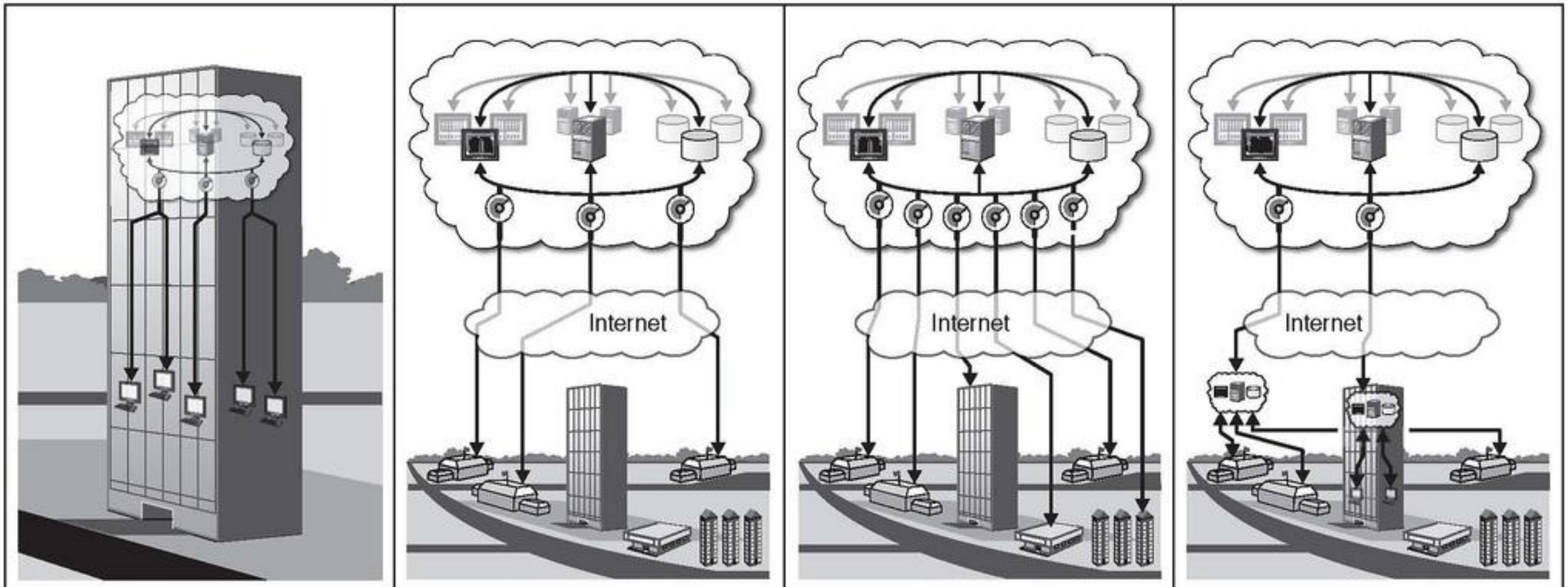
Infrastructure as a Service (IaaS)

Compute, storage or other IT infrastructure as a service, rather than as dedicated capability

TECHNICAL USE CASES & FAQS

Cloud Computing

Cloud Deployment Models



Private cloud
is operated solely for an organization and the cloud may be on or off the premises.

Community cloud
is shared by several organizations and supports a specific community of customers that have similar information technology requirements.

Public cloud
has an infrastructure that is made available to the general public or large industry group.

Hybrid cloud
has an infrastructure that is composed of two or more clouds that remain unique entities but are bound together by standardized or proprietary technology.

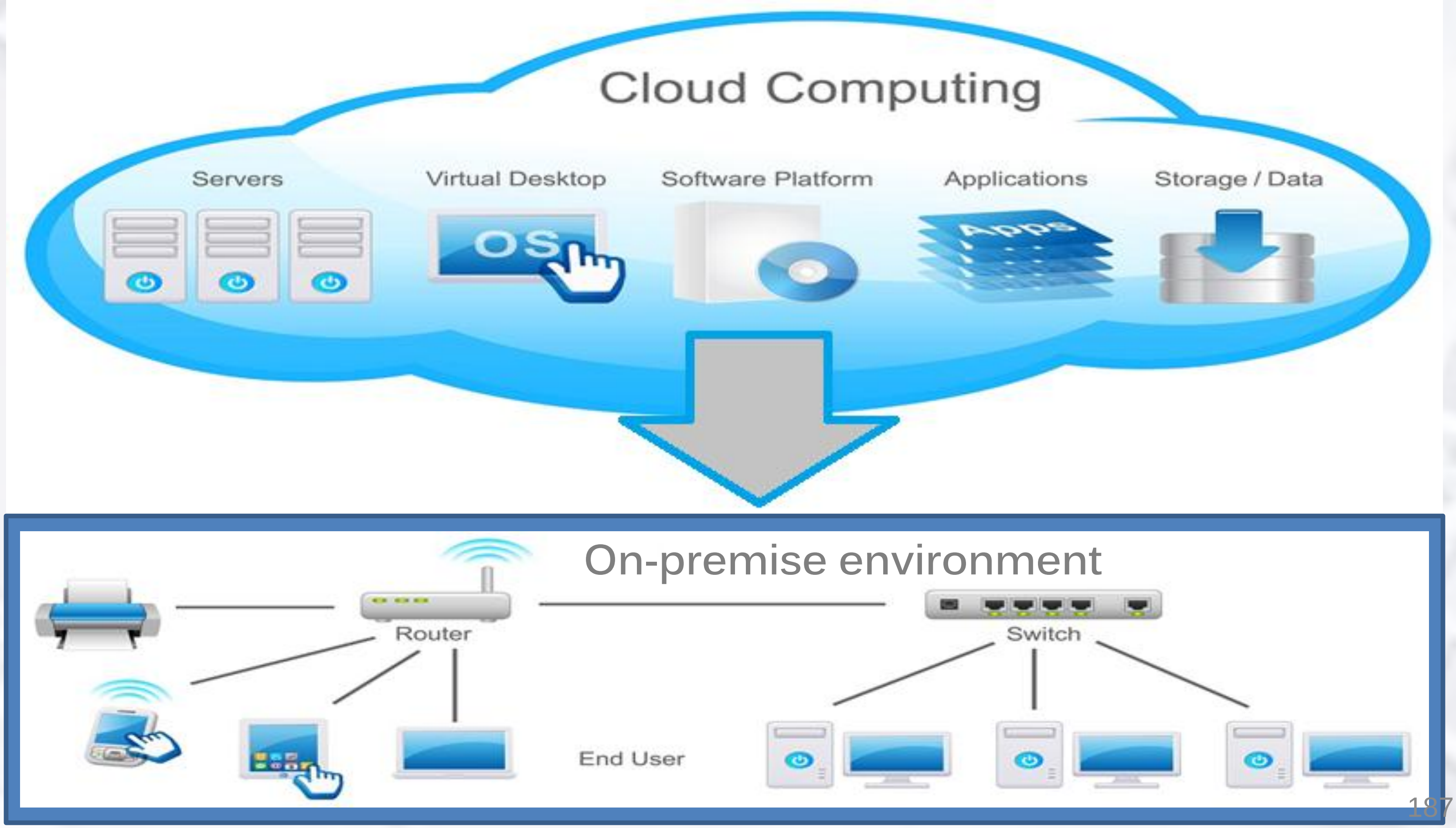
Cloud Computing

What Does a Cloud Deployment Actually Look Like?

TECHNICAL USE CASES & FAQS

Cloud Computing

This is a More Realistic Cloud Deployment Diagram



TECHNICAL USE CASES & FAQS

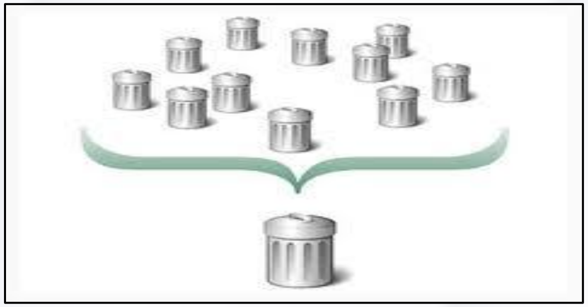
Cloud Computing

Benefits of Cloud Computing

Reduced Budgets

Improved Efficiency

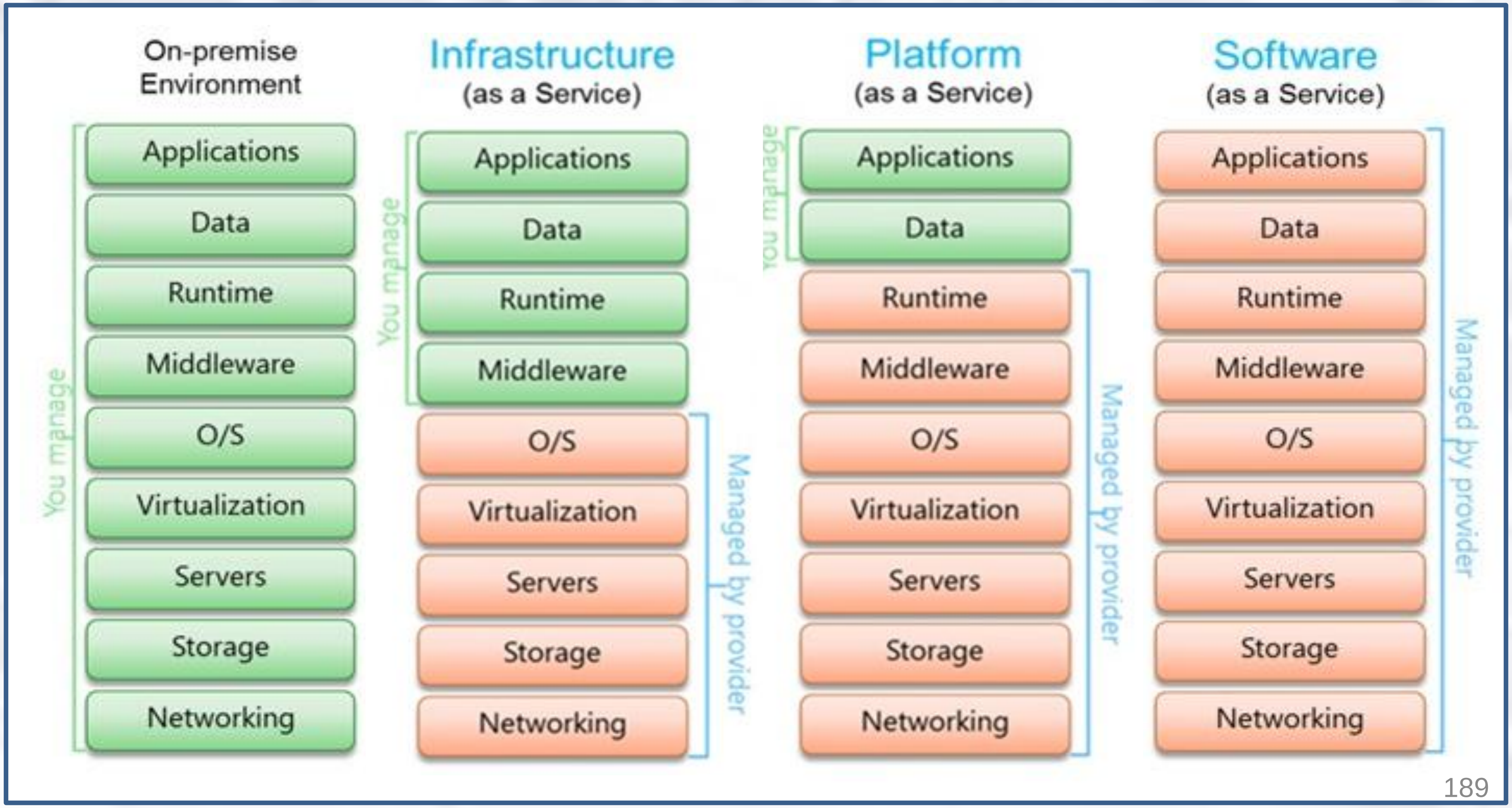
Disaster Recovery



Service Consolidation

Cloud Computing

Delineation of Responsibility/Governance in Cloud Computing



On-premise Environment	Infrastructure (as a Service)	Platform (as a Service)	Software (as a Service)
Applications	Applications	Applications	Applications
Data	Data	Data	Data
Runtime	Runtime	Runtime	Runtime
Middleware	Middleware	Middleware	Middleware
O/S	O/S	O/S	O/S
Virtualization	Virtualization	Virtualization	Virtualization
Servers	Servers	Servers	Servers
Storage	Storage	Storage	Storage
Networking	Networking	Networking	Networking

Cloud Computing

Security Concerns with Cloud Computing

- Privileged user access
- Regulatory compliance
- Data location
- Data segregation
- Recovery
- Investigative support
- Long-term viability

Cloud Computing

Cloud Computing and the CJIS Security Policy

- Section 5.10.1.5 Cloud Computing
  - ➢ The metadata derived from CJI shall not be used by any cloud service provider for any purposes.
  - ➢ The cloud service provider shall be prohibited from scanning any email or data files for the purpose of building analytics, data mining, advertising, or improving the services provided.
- Appendix G.3 Cloud Computing White Paper

Cloud Computing Use Case #1

Encryption for Data in the Cloud

- An NCJA decides to start utilizing cloud storage to backup files which do contain CJI.
- The agency encrypts the files using a FIPS 140-2 certified, 128 bit.
- Then, the agency sends the files to a cloud storage solution.
- The agency maintains the decryption passphrases so no cloud service provider will have access to unencrypted CJI.

Cloud Computing Use Case #2

Personnel Security for Cloud Service Provider

- A local PD is transitioning to a cloud-based virtualized network service and will permit the storage and transmission of CJI to/from the cloud.

- The cloud service provider as part of the service level agreement will provide encryption services for:
  - ➢ Data at rest (AES, 256 bit), and
  - ➢ An encrypted link for data in transit – TLS/SSL (FIPS 140-2 certified, 128 bit)

- This concept is not much different than outsourcing to a non-cloud provider. Any cloud service provider employee that has the capability of accessing the CJI in an unencrypted state (remember: cloud service provider is providing encryption services) must undergo a finger-print based background check, security awareness training, and sign the Security Addendum (SA)

Cloud Computing FAQ #1

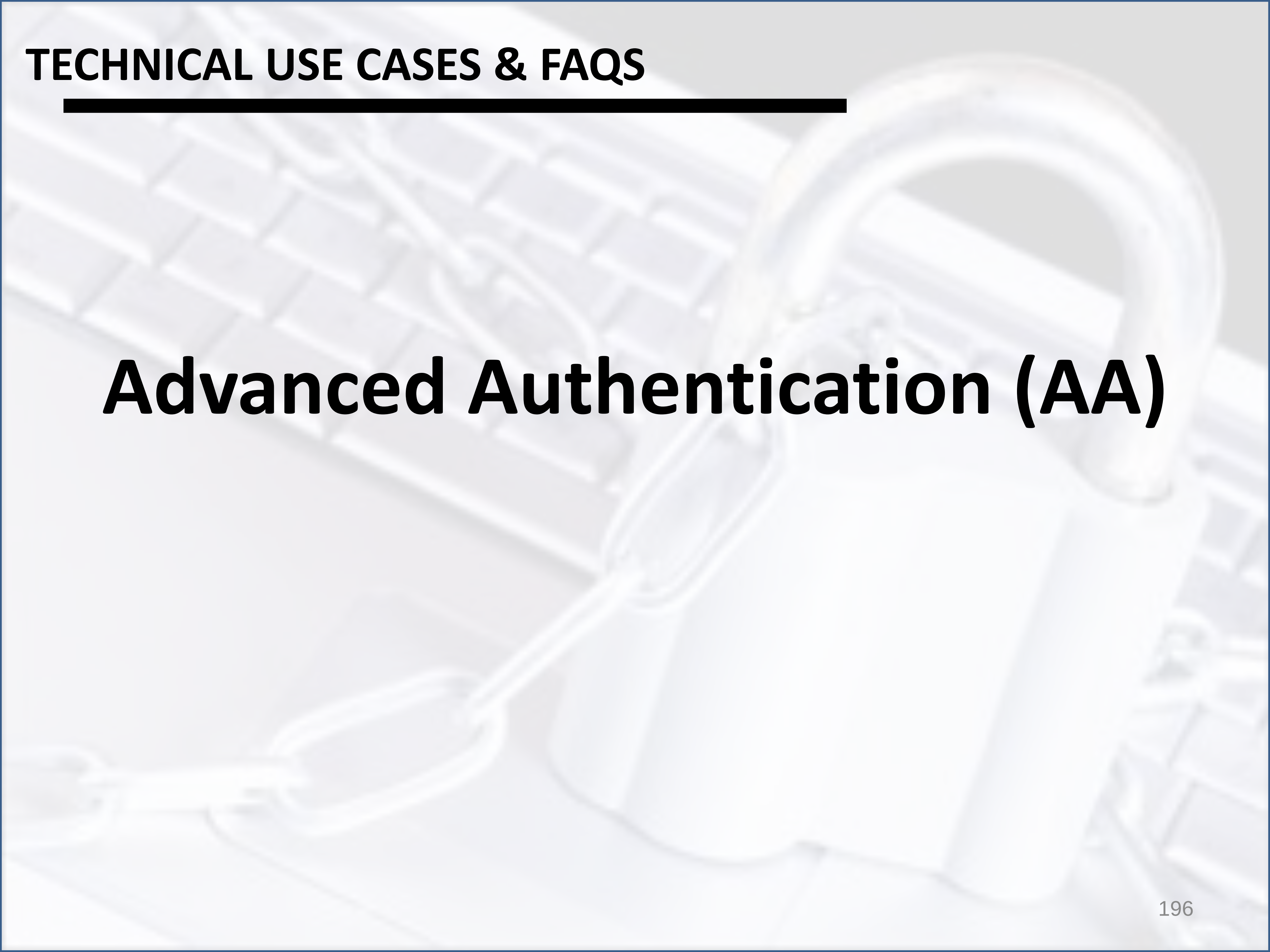
Question:
If our agency wants to store our backup data in a public cloud environment would we be required to have the cloud service provider (a private vendor) employees sign a Security Addendum and be subject to fingerprint-based background checks?

Answer:
Yes. The Security Addendum must be incorporated or referenced in the contract with the cloud service provider, and the Security Addendum Certificate pages must be signed by any and all cloud service provider employees who have access to unencrypted CJI. This ensures the provider agrees to abide by the requirements of the CJIS Security Policy (CSP) including submitting those cloud service provider employees (with access to the unencrypted CJI) for a fingerprint-based background check.

Cloud Computing FAQ #2

Question:
Our city has recently been considering moving to cloud-based email service covering all city departments and agencies, to include the local police department. Our question is: Are we allowed to send criminal justice information (CJI) through email?

Answer:
You can send e-mail containing Criminal Justice Information (CJI) as long as it remains within your physically secure environment (as described in the Policy), you send the e-mail along an encrypted path (FIPS 140-2 certified, 128 bit) to the recipient, or you encrypt (FIPS 140-2 certified, 128 bit) the payload of an e-mail.



Advanced Authentication (AA)

Advanced Authentication (AA)

When AA is Required

Required:

✓ When requesting access to unencrypted CJI from outside the boundaries of a physically secure location (e.g., remote access)

Or

✓ Technical security requirements for a physically secure location have not been met

Not required:

x When requesting access to CJI from within the perimeter of a physically secure location

And

x The technical security controls have been met

Or

x User has indirect access CJI

TECHNICAL USE CASES & FAQS

Advanced Authentication (AA)

The Purpose of AA

- To provide additional assurance the user is who they claim to be.
  - ➢ Authorized User?

- AA provides additional security beyond the typical user identification (e.g., user ID) and authentication (e.g., password):
  - ➢ Increased Assurance of User Identity
  - ➢ Non-repudiation
  - ➢ Lower Risk for Data Exfiltration

Advanced Authentication (AA)

Achieving AA

- The intent of AA is to meet the standards of two-factor authentication.
- Authenticators provide the “something you know”, “something you are”, or “something you have” within a two factor authentication solution.
- A Risk-based Authentication (RBA) solution can be used to provide one of the authenticators.
- **The AA equation:**
  (ID) + (authenticator 1) + (authenticator 2) = AA

TECHNICAL USE CASES & FAQS

Advanced Authentication (AA)

Proper Implementation of AA

- Each individual’s identity shall be authenticated at either the local agency, CSA, SIB or Channeler level.
- The authentication strategy shall be part of the agency’s audit for policy compliance.
  - ➢ The credentials used for determining CJI access will be audited for CJIS Security Policy compliance.
- Users cannot use the same password or PIN in the same logon sequence.

Advanced Authentication (AA) Use Case #1

Use of a Smart Card – PKI solution using user-based certificates

- Using a terminal within a controlled area, the user launches an NCIC application to run a CJI query.
- When prompted, the user enters a username, password, and inserts the smart card – user is required to enter a PIN to unlock (or activate) the smart card to allow the use of the digital user certificate.
- The credentials are sent to the authentication management server at the local agency where they are validated. And access is granted.
- **The AA equation**: username (ID) + password (“something you know”) + digital user certificate (“something you have”) = AA

Advanced Authentication (AA) Use Case #2

Out of Band One-Time-Password (OTP) – Mobile phone-based

- A user established a remote connection to the agency network via an encrypted (FIPS 140-2 certified, 128 bit) virtual private network (VPN) connection.
- Upon establishing the VPN, the user is prompted to enter a username and password. Then, a text message containing a one-time password (OTP) is sent via text message (out of band) to the user's agency-issued cell phone.
- The user enters the OTP.
- The credentials are sent to the authentication management server at the local agency where they are validated. And access is granted.
- **The AA equation**: username (ID) + password ("something you know") + OTP ("something you have") = AA

Advanced Authentication (AA) FAQ #1

Question:
If I am using a computing device from within my police vehicle, do I need AA?

Answer:
Maybe. There are technical controls (Sections 5.5. & 5.10) that have to be met as with any physically secure location. Additionally, you must be able to know the originating CJI request came from within a police vehicle (physically secure location).

If a device (e.g., laptop, tablet, smartphone) is not mounted in the vehicle and is usable while mobile outside of the vehicle, then the location of the query cannot be positively determined. Therefore, AA would be requirement.

Advanced Authentication (AA) FAQ #2

Question:

We use live scan devices at our agency to collect and submit fingerprints. Officer swipes a subjects fingerprint through the scanner. The data is sent to the national database for analysis. Is AA required on these devices?

Answer:

If CJI is returned to the scanner and the request for access can be determined to have originated from within a physically secure location then AA isn't required. Otherwise, AA would be required due to device location and CJI being sent to the device.

Conversely, If the scanner is only used to submit data (regardless of location) or only receive a hit/no hit or red/green light response, then AA would not be required.

TECHNICAL USE CASES & FAQS

Questions?

BREAK

“On the Horizon”

Jeff Campbell

FBI CJIS Assistant Information Security Officer

ON THE HORIZON

- Encryption Exemption
- Requirement Tiering
- Certificate Use Clarification
- Partitioning and Virtualization
- Virtual Escorting
- In/Out-of-band Clarification
- Auditing Facilities in Other Jurisdictions
- Policy Area 13: Mobile Devices Update
- Mobile Appendix Update
- Cloud Appendix Update
- Faxing Requirements Update
- Appendix K Value

ON THE HORIZON

Title: **Exception to CJIS Security Policy Section 5.10.1.2 Exemptions**

Current Status: Being presented to the Fall 2014 Working Groups for action

Physical or technical controls to allow cabling carrying unencrypted CJI between physically secure locations.

ON THE HORIZON

Title: **Integrating Risk-based Compliance and Requirement Tiering into the CJIS Security Policy**

Current Status: Being presented to the Fall 2014 Working Groups for action

Final stages of determining if and how to integrate requirement tiers into the Policy.

ON THE HORIZON

Title: **Clarifying Types of Certificates**

Current Status: Being presented to the Fall 2014 Working Groups for action

Propose modification to the CJIS Security Policy to clarify the use of certificates, especially in the advanced authentication process.

ON THE HORIZON

Title: **Clarification of Virtualization and Partitioning in the CJIS Security Policy**

Current Status: Being presented to the Fall 2014 Working Groups for action

Present recommended changes to the Policy to clarify the practice of virtualization and partitioning.

ON THE HORIZON

Title: **Virtual Escorting**

Current Status: Being presented to the Fall 2014 Working Groups for action

Identify a method to virtually escort a remote session for system maintenance.

ON THE HORIZON

Title: **In/Out-of-Band Clarification**

Current Status: Ad Hoc preparation with SA Subcommittee. Planned for Spring 2015 Working Groups for action.

Add or modify Policy language to clarify the meaning of in/out-of-band use of supplying logon credentials.

ON THE HORIZON

Title: **Auditing Facilities in Other Jurisdictions**

Current Status: Topic paper request received and topic being developed for Spring 2015 Working Groups.

This topic will focus on discussing how to modify the CJIS Security Policy to allow a CSA to perform facility inspections of vendors that are in a different state.

ON THE HORIZON

Title: **Update Policy Area 13: Mobile Devices**

Current Status: Topic paper request submitted by Mobile Security Task Force chairman

During the process to modify the Policy with the mobile updates, a Mobile Security Task Force was created to review mobile-centric topics and provide recommendations to the Security and Access Subcommittee. The task force reviewed the proposed changes and will make recommendations for modifying the Policy.

ON THE HORIZON

Title: **Mobile Appendix Update**

Current Status: In development – target Spring 2015
Working Groups

The FBI CJIS ISO Program is developing an update to the Mobile Appendix - bringing the information up to current industry best practices.

ON THE HORIZON

Title: **Cloud Appendix Update**

Current Status: Being considered

The FBI CJIS ISO is considering an update to the Cloud Appendix to level the information with current industry best practices.

ON THE HORIZON

Title: **Faxing Requirements Update**

Current Status: Draft

Update the language in Section 5.10.2 to keep pace with new fax technology such as fax servers or web based fax services that essentially function as email.

ON THE HORIZON

Title: **Appendix K Value**

Current Status: Draft

Review Appendix K and determine if it still provides value as a tool to criminal justice agencies with respect to the CJIS Security Policy requirements.

ON THE HORIZON

Questions?

ISO RESOURCES

CJIS Security Policy Resource Center

- Publically Available:

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

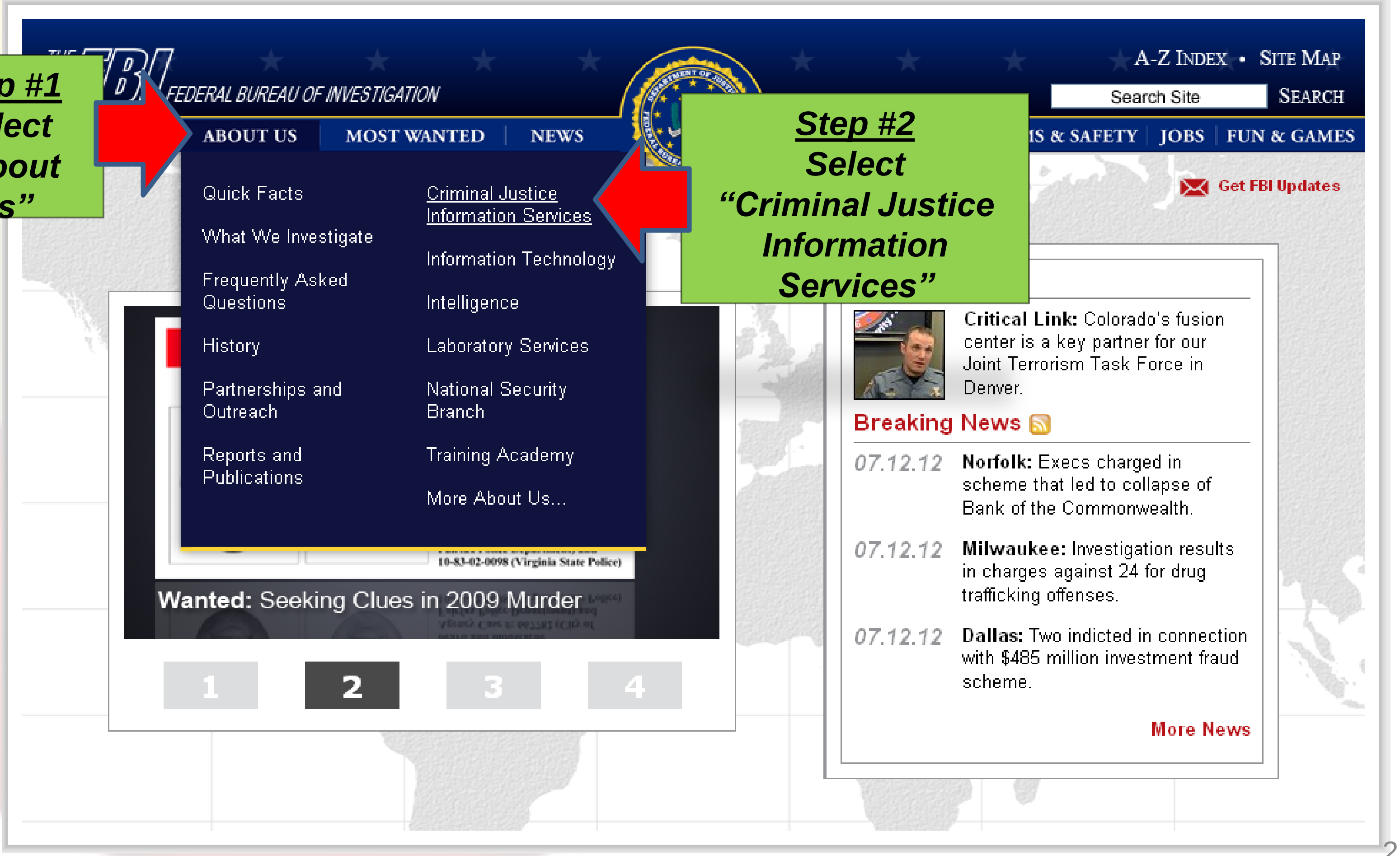
- Features:
  - Search and download the CSP
  - Download the CSP Requirements and Transition Document
  - Use Cases (Advanced Authentication and others to follow)
  - Cloud Computing Report & Cloud Report Control Catalog
  - Mobile Appendix
  - Submit a Question (question forwarded to CJIS ISO Program)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

iso@leo.gov

ISO RESOURCES

CJIS Security Policy Resource Center

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



Step #1
Select "About Us"

Step #2
Select "Criminal Justice Information Services"

Wanted: Seeking Clues in 2009 Murder

Critical Link: Colorado's fusion center is a key partner for our Joint Terrorism Task Force in Denver.

Breaking News

07.12.12 **Norfolk:** Execs charged in scheme that led to collapse of Bank of the Commonwealth.

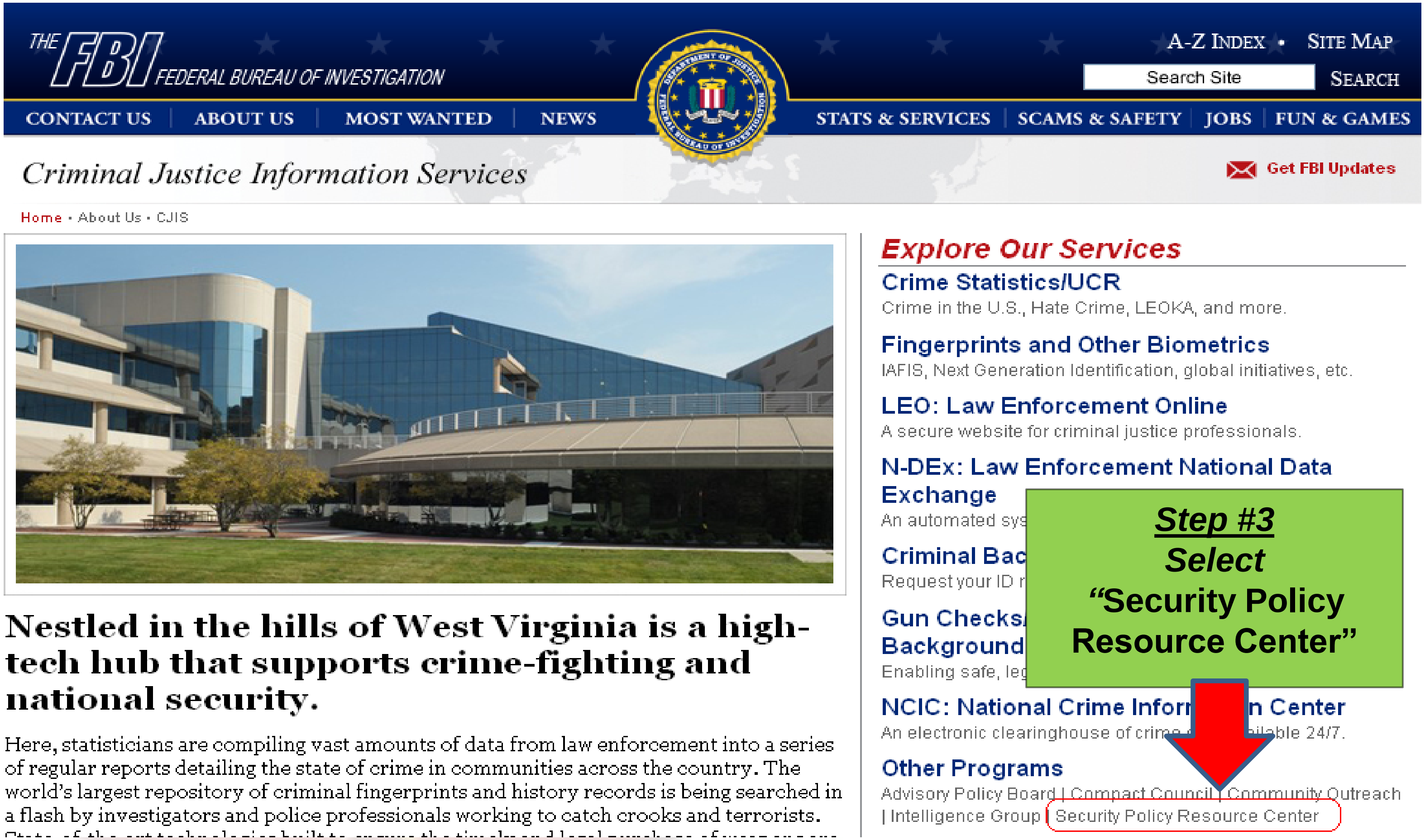
07.12.12 **Milwaukee:** Investigation results in charges against 24 for drug trafficking offenses.

07.12.12 **Dallas:** Two indicted in connection with $485 million investment fraud scheme.

ISO RESOURCES

CJIS Security Policy Resource Center

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



Criminal Justice Information Services

Nestled in the hills of West Virginia is a high-tech hub that supports crime-fighting and national security.

Here, statisticians are compiling vast amounts of data from law enforcement into a series of regular reports detailing the state of crime in communities across the country. The world's largest repository of criminal fingerprints and history records is being searched in a flash by investigators and police professionals working to catch crooks and terrorists.

Explore Our Services

Crime Statistics/UCR
Crime in the U.S., Hate Crime, LEOKA, and more.

Fingerprints and Other Biometrics
IAFIS, Next Generation Identification, global initiatives, etc.

LEO: Law Enforcement Online
A secure website for criminal justice professionals.

N-DEx: Law Enforcement National Data Exchange
An automated sys

Criminal Bac
Request your ID r

Gun Checks/ Background
Enabling safe, leg

NCIC: National Crime Infor n Center
An electronic clearinghouse of crime ilable 24/7.

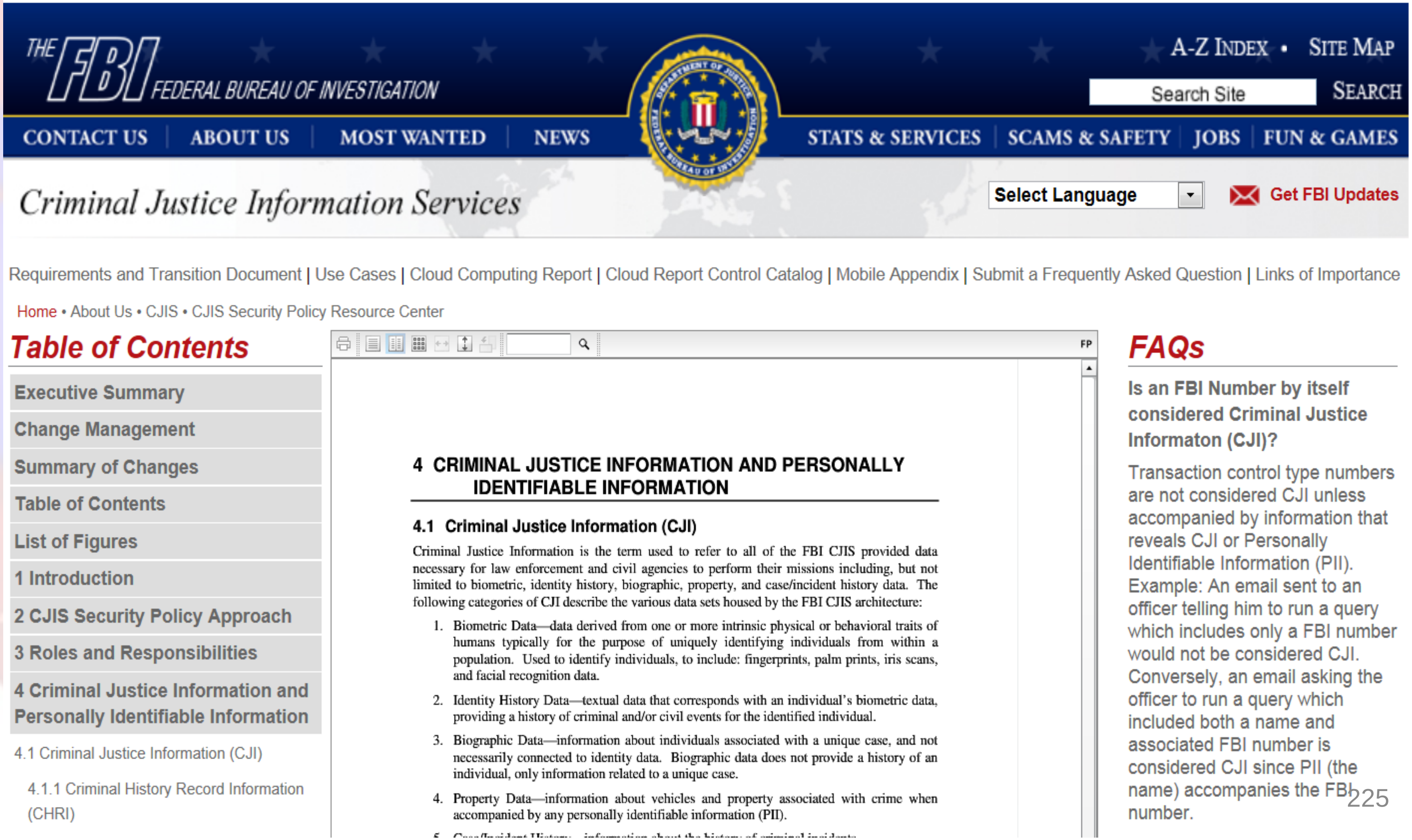
Other Programs
Advisory Policy Board | Compact Council | Community Outreach | Intelligence Group | Security Policy Resource Center

Step #3
Select
"Security Policy Resource Center"

ISO RESOURCES

CJIS Security Policy Resource Center

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



THE FBI FEDERAL BUREAU OF INVESTIGATION
A-Z INDEX • SITE MAP
Search Site
SEARCH
CONTACT US | ABOUT US | MOST WANTED | NEWS
STATS & SERVICES | SCAMS & SAFETY | JOBS | FUN & GAMES
Criminal Justice Information Services
Select Language
Get FBI Updates
Requirements and Transition Document | Use Cases | Cloud Computing Report | Cloud Report Control Catalog | Mobile Appendix | Submit a Frequently Asked Question | Links of Importance
Home • About Us • CJIS • CJIS Security Policy Resource Center
FP

Table of Contents

4 CRIMINAL JUSTICE INFORMATION AND PERSONALLY IDENTIFIABLE INFORMATION

4.1 Criminal Justice Information (CJI)

Criminal Justice Information is the term used to refer to all of the FBI CJIS provided data necessary for law enforcement and civil agencies to perform their missions including, but not limited to biometric, identity history, biographic, property, and case/incident history data. The following categories of CJI describe the various data sets housed by the FBI CJIS architecture:

1. Biometric Data—data derived from one or more intrinsic physical or behavioral traits of humans typically for the purpose of uniquely identifying individuals from within a population. Used to identify individuals, to include: fingerprints, palm prints, iris scans, and facial recognition data.
2. Identity History Data—textual data that corresponds with an individual's biometric data, providing a history of criminal and/or civil events for the identified individual.
3. Biographic Data—information about individuals associated with a unique case, and not necessarily connected to identity data. Biographic data does not provide a history of an individual, only information related to a unique case.
4. Property Data—information about vehicles and property associated with crime when accompanied by any personally identifiable information (PII).
5. Case/Incident History—information about the history of criminal incidents

FAQs

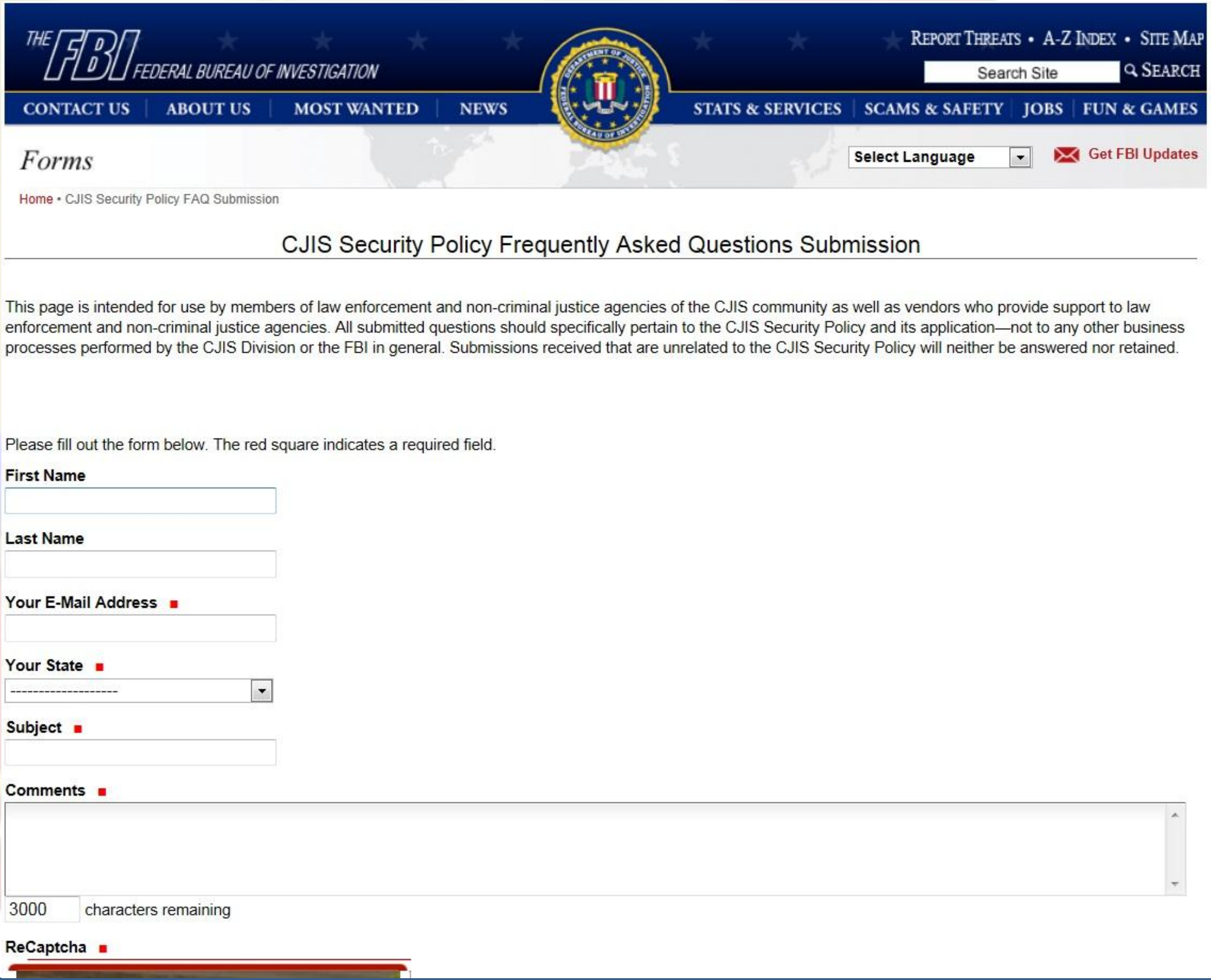
Is an FBI Number by itself considered Criminal Justice Informaton (CJI)?

Transaction control type numbers are not considered CJI unless accompanied by information that reveals CJI or Personally Identifiable Information (PII). Example: An email sent to an officer telling him to run a query which includes only a FBI number would not be considered CJI. Conversely, an email asking the officer to run a query which included both a name and associated FBI number is considered CJI since PII (the name) accompanies the FBI number.

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 ■

Open Forum Discussion

George White
FBI CJIS Information Security Officer
Chief, CJIS Information Assurance Unit

Closing Remarks

George White

FBI CJIS Information Security Officer

Chief, CJIS Information Assurance Unit

DINNER

On Your Own

Peer-to-Peer Discussions

George White

FBI CJIS Information Security Officer

Chief, CJIS Information Assurance Unit

Closing Remarks

George White

FBI CJIS Information Security Officer

Chief, CJIS Information Assurance Unit