# CJIS Security Policy Updates

TAC Conference 2023

# Agenda

- Overview of CJIS Security Policy Changes
- Security Awareness and Training Updates
- Role - Based Training Content
- TAC Next Steps

# Updates

# APB Approved Changes

## Section 5.2

Modernization of Awareness Training in CJISSECPOL

## Section 5.6

Modernization of Identification and Authentication in CJISSECPOL

## Section 5.14

Update CJIS Security Policy for Unsupported System Components

## Section 5.15

Modernization of System and Information Integrity in CJISSECPOL

# Administrative Changes

## Section 5.8

Modernization of Discussion to Include Community - Relevant Example of Access to Non - Digital Media

## Appendix A Terms and Definitions

Include Definition for "Non - Digital Media"

# Section 5.2

Awareness and Training (AT)

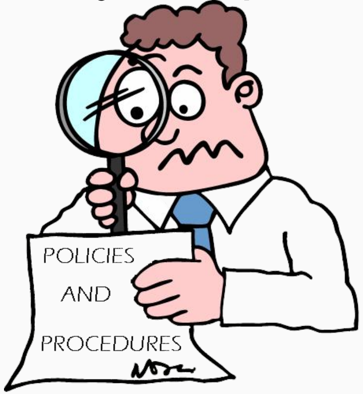
- AT- 1
- AT- 2
- AT- 3
- AT- 4

# 5.2 Awareness and Training (AT)

Security training is key to the human element of information security. All users with authorized access to CJI should be made aware of their individual responsibilities and expected behavior when accessing CJI and the systems which process CJI. LASOs require enhanced training on the specific duties and responsibilities of those positions and the impact those positions have on the overall security of information systems.

# AT- 1: Policy and Procedures

- Agencies must:
    - Develop, document, and disseminate awareness and training policy and procedures
    - Manage the development, documentation, and dissemination of the awareness and training policy and procedures
    - Review and update policy and procedures



# AT- 1: Policy and Procedures

- Organization level awareness and training policy
  - Purpose
  - Scope
  - Responsibilities
  - Management commitment
  - Coordination among organizational entities
  - Compliance
  - Consistent with applicable laws, executive orders, directives, regulations, policies, standards and guidelines
- Procedures to implement policy

# AT- 1: Policy and Procedures

- Manage the development, documentation, and dissemination of the awareness and training policy and procedures
  - Designate personnel

# AT- 1: Policy and Procedures

- Review and update the current awareness and training policy and procedures annually and following any changes to:
    - CJIS Security Policy
    - Information system operating environment
    - When security incidents occur

# AT- 1: Policy and Procedures

- What does this mean for you?
  - Develop and implement policy and procedure
    - Can be included as part of your agency's general security and privacy policy
    - Can be represented by multiple policies
  - Procedures can be documented in system security and privacy plans
    - Can be in one or more separate documents
  - Review and update policy and procedures annually

# AT- 2: Literacy Training and Awareness

- Provide the following:
    - Security and privacy literacy training to system users
    - Literacy training on recognizing and reporting potential indicators of insider threat
    - Literacy training on recognizing and reporting potential and actual instances of social engineering and social mining

# AT-2: Literacy Training and Awareness

- Provide security and privacy literacy training to system users
  - Includes managers, senior executives, and contractors
  - As part of initial training and **annually** thereafter
  - When required by system changes or within 30 days of any security event for individuals involved in the event

Privacy & Security Training

BCI has updated the Privacy & Security training on the TAC website. This will be live on October 1, 2023. This can be used for security awareness training for all user types, however it shouldn't be the main source for security awareness training. You must have your own training tools that you use and update annually per CJIS Policy AT-2.

# AT-2: Literacy Training and Awareness

- Increase security and privacy awareness of system users by:
  - Displaying posters
  - Offer supplies with security and privacy reminders inscribed
  - Display logon screen messages
  - Emails
  - Awareness events
- Update content annually and following changes in CJIS Policy, information system operating environment, and when incidents occur
- Use internal or external incidents as examples

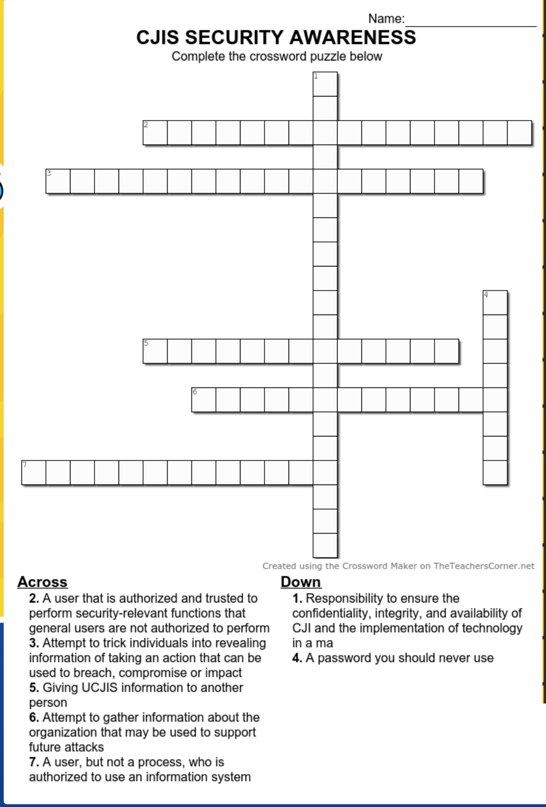
# ATTENTION

Security Awareness Week

October 23-27, 2023

WE WILL SEND OUT DAILY FACTS & HAVE SOME GAMES

PARTICIPATION IS REQUIRED



Name:____________________

## CJIS SECURITY AWARENESS

Complete the crossword puzzle below

Created using the Crossword Maker on TheTeachersCorner.net

**Across**

**2.** A user that is authorized and trusted to perform security-relevant functions that general users are not authorized to perform

**3.** Attempt to trick individuals into revealing information of taking an action that can be used to breach, compromise or impact

**5.** Giving UCJIS information to another person

**6.** Attempt to gather information about the organization that may be used to support future attacks

**7.** A user, but not a process, who is authorized to use an information system

**Down**

**1.** Responsibility to ensure the confidentiality, integrity, and availability of CJI and the implementation of technology in a ma

**4.** A password you should never use

# WORKPLACE SECURITY

Public must not be able to see information

Make sure you keep print outs in a secure area

Vistors must be accompanied at all times

Make sure you have your badge and keycard with you at all times

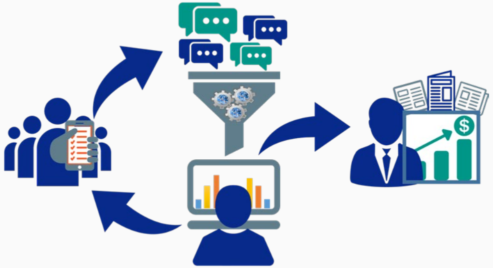
IMPORTANT

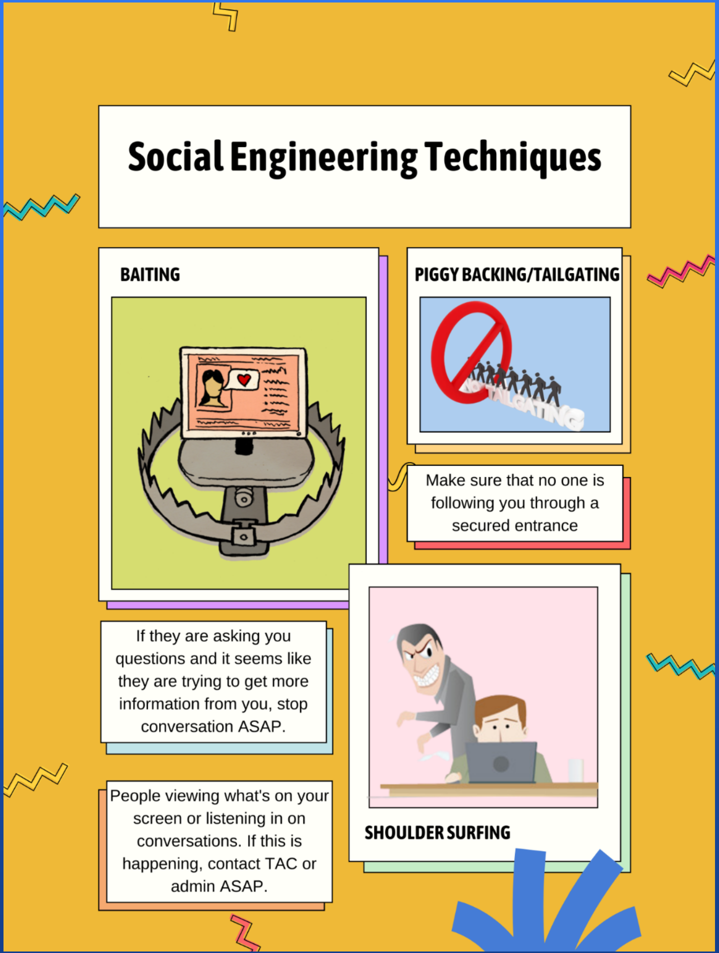
# AT-2: Literacy Training and Awareness

- Provide literacy training on recognizing and reporting potential indicators of insider threat
  - Potential indicators
    - Inordinate, long - term job dissatisfaction
    - Attempts to obtain information not related to job
    - Unexplained access
    - Workplace violence
  - Tailor insider threat awareness topics to the role
    - Training for managers may be focused on changes in the behavior of team members
    - Training for employees may be focused on general observations

# AT-2: Literacy Training and Awareness

- Provide literacy training on recognizing and reporting potential and actual instances of social engineering and social mining
  - Social engineering
    - Attempt to trick individuals into revealing  information of taking an action that can be used to breach, compromise or impact a system
  - Social mining
    - Attempt to gather information about the organization that may be used to support future attacks





# Social Engineering Techniques

## BAITING

If they are asking you questions and it seems like they are trying to get more information from you, stop conversation ASAP.

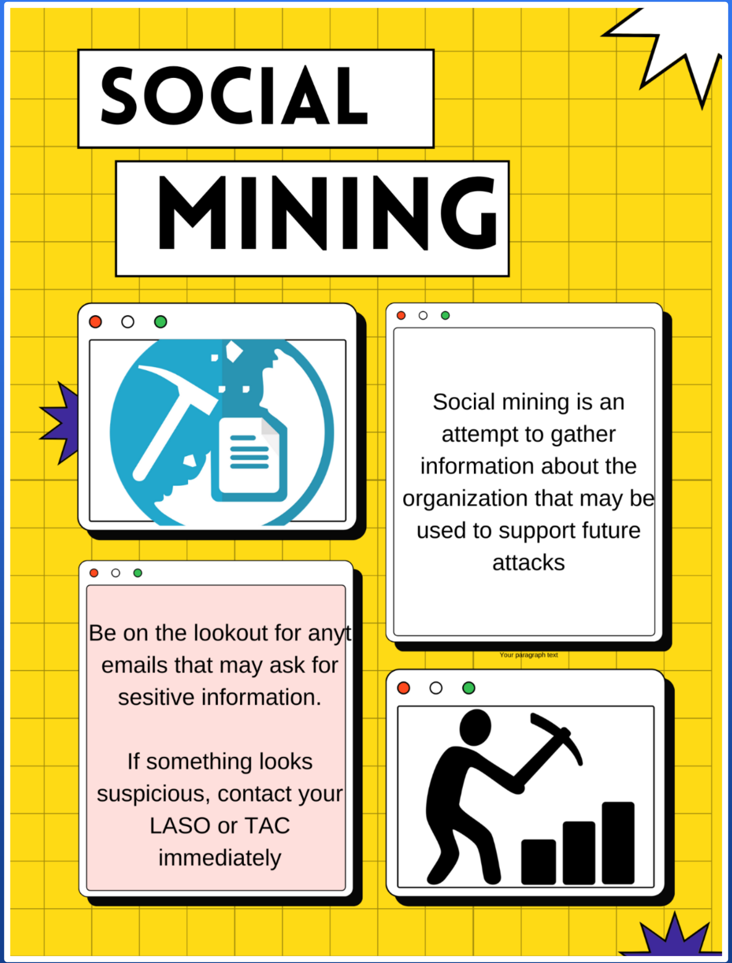
## PIGGY BACKING/TAILGATING

NO TAILGATING

Make sure that no one is following you through a secured entrance

## SHOULDER SURFING

People viewing what's on your screen or listening in on conversations. If this is happening, contact TAC or admin ASAP.



# SOCIAL MINING

Social mining is an attempt to gather information about the organization that may be used to support future attacks

Your paragraph text

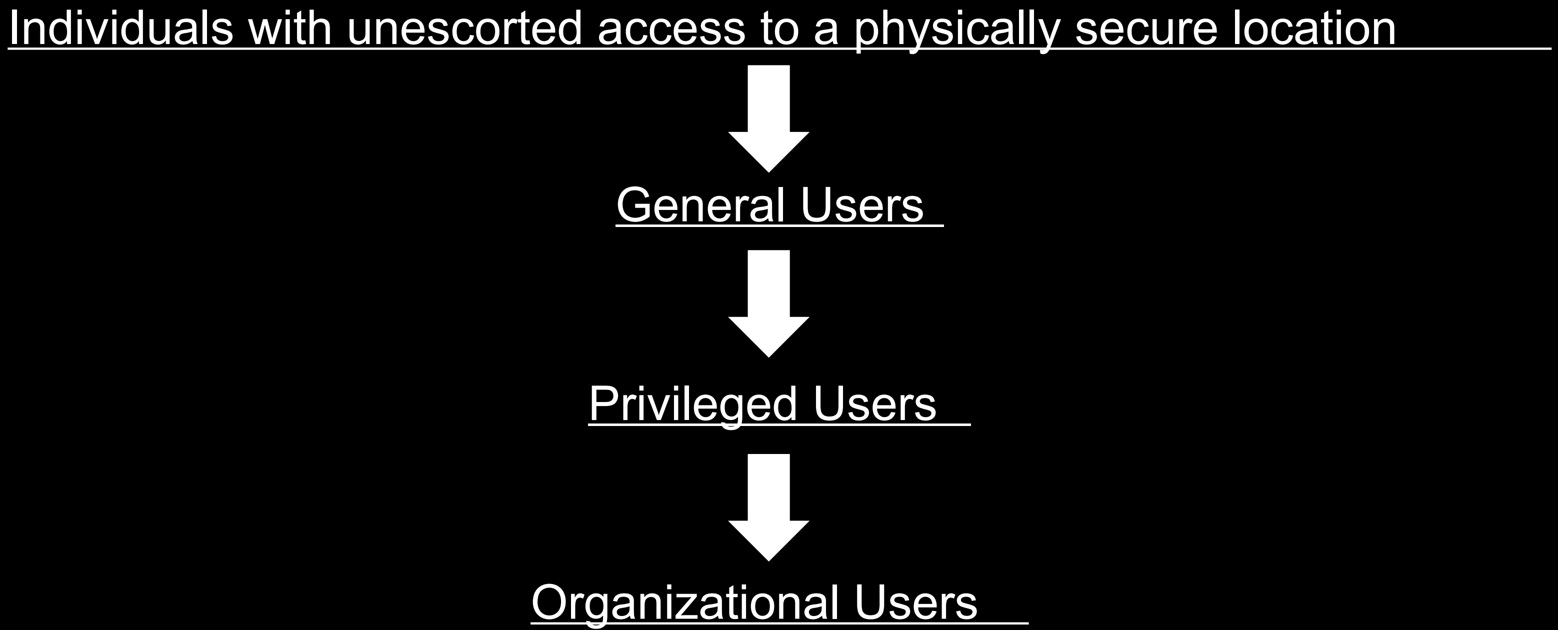
Be on the lookout for anyt emails that may ask for sesitive information.

If something looks suspicious, contact your LASO or TAC immediately

# AT-3: Role-Based Training

- Provide role - based security and privacy training to personnel with the following roles and responsibilities:
  - **Individuals with unescorted access to a physically secure location**
  - **General users**
  - **Privileged users**
  - **Organizational personnel with security responsibilities**

# Role-Based Training Chain



Individuals with unescorted access to a physically secure location

General Users

Privileged Users

Organizational Users

# AT-3: Role-Based Training (*continued*)

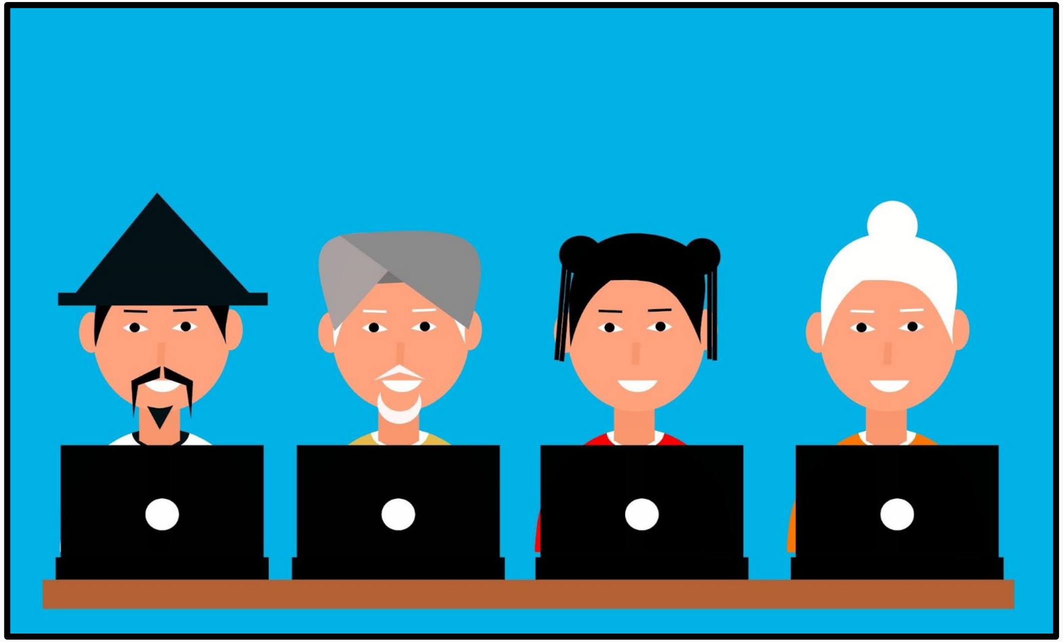
- All individuals with unescorted access to a physically secure location.

# AT-3: Role-Based Training (*continued*)

- In BCI Language
  - Access Levels
    - *Non-User*

# AT-3: Role-Based Training (*continued*)

- General User: A user, but not a process, who is authorized to use an information system.



# AT-3: Role-Based Training (*continued*)

- In BCI Language
    - Access Levels
        - *User*
        - *Non-Access User*

# AT-3: Role-Based Training (*continued*)

- In BCI Language
  - *Manager*
  - *Supervisor*
  - *Senior Executive*

# AT-3: Role-Based Training (*continued*)

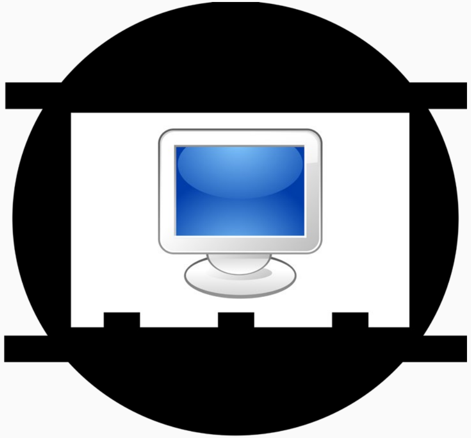
- Privileged User: A user that is authorized and trusted to perform security-relevant functions that general users are not authorized to perform.

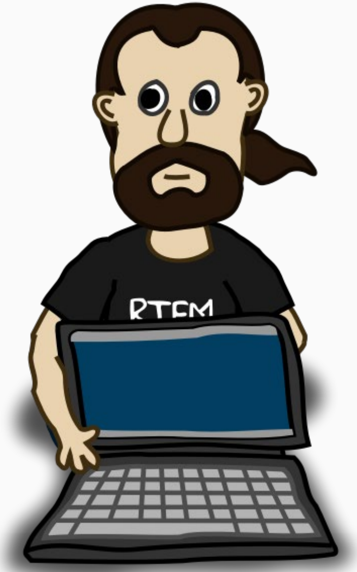
# AT-3: Role-Based Training (*continued*)

- In BCI Language
  - *System Programmer*
  - *Security Administrator*
  - *System and Network Administrator*
  - *Information System Security Officer*
    - *CJIS Systems Officer (CSO)*

# AT-3: Role-Based Training (*continued*)

- Organizational Personnel with Security Responsibilities: Responsibility to ensure the confidentiality, integrity, and availability of CJI and the implementation of technology in a manner compliant with the CJISSECPOL.
  - Manage the development, documentation, and dissemination of the awareness and training policy and procedures.





# AT-3: Role-Based Training (*continued*)

- In BCI Language
  - *Contractor*
  - *Guest Researcher*
  - *Local Agency Security Officer (LASO)*

# AT-4: Training Records

- Document and monitor information security and privacy training activities
  - security and privacy awareness training
  - specific role - based security and privacy training
- Retain individual training records for a minimum of three years.

# Security Awareness Training Use Case #1

A local police department hires custodial staff that will have physical access throughout the police department (a physically secure location) after normal business hours to clean the facility.

Who does this apply to?

A. General Users

B. Privileged Users

C. Organizational Users

D. Individuals with unescorted access to a physically secure location

# Security Awareness Training Use Case #1

A local police department hires custodial staff that will have physical access throughout the police department (a physically secure location) after normal business hours to clean the facility.

Who does this apply to?

A. General Users
B. Privileged Users
C. Organizational Users
D. **Individuals with unescorted access to a physically secure location**

# Individuals with unescorted access to a physically secure location

- Visitor Control
- Reporting Security Events
- Access, Use and Dissemination of CHRI and NCIC files
- System Use Notification
- Physical Access Control
- Incident Response Training

# Security Awareness Training Use Case #2

A school district maintains a locked file cabinet with hard copies of background check results of all teachers and employees which may include CJI (CHRI). Only authorized personnel have the ability to open the cabinet.

Who does this apply to?

A. General Users

B. Privileged Users

C. Organizational Users

D. Individuals with unescorted access to a physically secure location

# Security Awareness Training Use Case #2

A school district maintains a locked file cabinet with hard copies of background check results of all teachers and employees which may include CJI (CHRI). Only authorized personnel have the ability to open the cabinet.

Who does this apply to?

A. **General Users**

B. Privileged Users

C. Organizational Users

D. Individuals with unescorted access to a physically secure location

# General Users

- System Access Control
- Proper Handling & Storage
- Literacy Training and Awareness
- Criminal Justice Information
- Passwords and Encryption
- Security, Protection and Management of Devices

# Security Awareness Training Use Case #3

State Police hired system and network administrator personnel to help bolster security of the state network. Part of their daily duties may include creating accounts for new personnel, implementing security patches and creating backups for existing systems, and implementing access controls throughout the network.

Who does this apply to?

A. General Users
B. Privileged Users
C. Organizational Users
D. Individuals with unescorted access to a physically secure location

# Security Awareness Training Use Case #3

State Police hired system and network administrator personnel to help bolster security of the state network. Part of their daily duties may include creating accounts for new personnel, implementing security patches and creating backups for existing systems, and implementing access controls throughout the network.

Who does this apply to?

A. General Users

**B. Privileged Users**

C. Organizational Users

D. Individuals with unescorted access to a physically secure location

# Privileged Users

- Patch Management
- Data Backup and Storage
- System and Communications Protection
- Access Control
- CJIS Security Policy Changes
- Information Integrity

# Security Awareness Training Use Case #4

A County Sheriff's Office employs a private contractor to perform criminal justice functions on behalf of their police department. The contractor is responsible for managing the development, documentation, and dissemination of the awareness and training policy and procedures.

Who does this apply to?

A. General Users

B. Privileged Users

C. Organizational Users

D. Individuals with unescorted access to a physically secure location

# Security Awareness Training Use Case #4

A County Sheriff’s Office employs a private contractor to perform criminal justice functions on behalf of their police department. The contractor is responsible for managing the development, documentation, and dissemination of the awareness and training policy and procedures.

Who does this apply to?

A. General Users

B. Privileged Users

**C. Organizational Users**

D. Individuals with unescorted access to a physically secure location

# Organizational Users

- LASO Role
- State Audit Findings
- State/local/tribal agency roles & responsibilities

- ARSO Role
- FBI CJIS Audit Findings
- Federal agency roles & responsibilities

# Steps that Follow

# APB Approved Changes

## Section 5.6

Modernization of Identification and Authentication in CJISSECPOL

## Section 5.14

Update CJIS Security Policy for Unsupported System Components

## Section 5.15

Modernization of System and Information Integrity in CJISSECPOL

# Section 5.6

## Identification and Authentication (IA)

- IA - 0
- IA - 1
- IA - 2
- IA - 3
- IA - 4
- IA - 5
- IA - 6
- IA - 7
- IA - 8
- IA - 11
- IA - 12

# Section 5.14

System and Services Acquisition (SA)

- Unsupported System Components

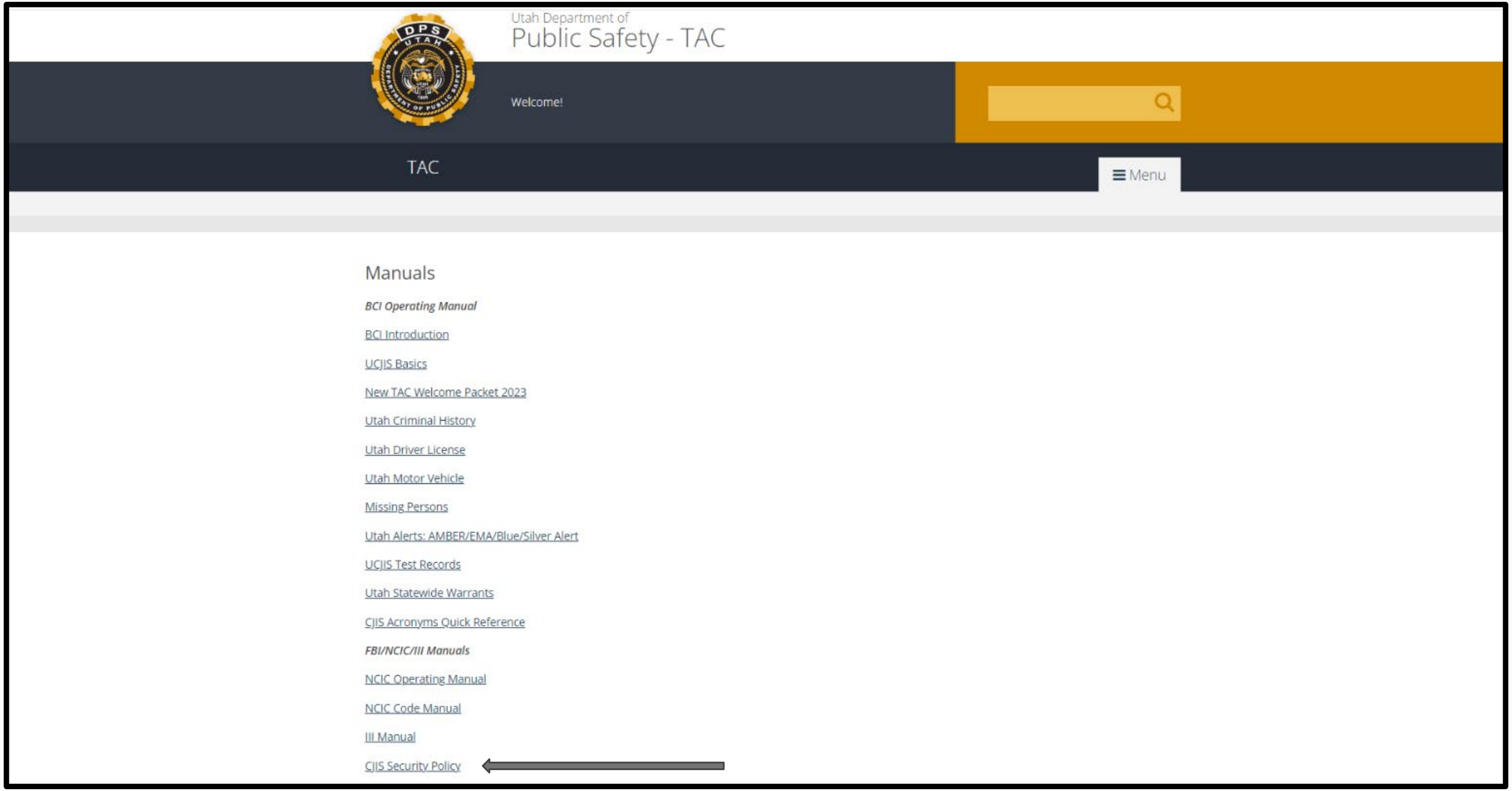
# Section 5.15

## System and Information Integrity (SI)

- SI- 1
- SI- 2
- SI- 3
- SI- 4
- SI- 5
- SI- 7
- SI- 8
- SI- 10
- SI- 11
- SI- 12
- SI- 16

# October 1, 2023

Requirements sanctionable for audit beginning on this date



Utah Department of
Public Safety - TAC

Welcome!

TAC

Manuals

*BCI Operating Manual*

BCI Introduction

UCJIS Basics

New TAC Welcome Packet 2023

Utah Criminal History

Utah Driver License

Utah Motor Vehicle

Missing Persons

Utah Alerts: AMBER/EMA/Blue/Silver Alert

UCJIS Test Records

Utah Statewide Warrants

CJIS Acronyms Quick Reference

*FBI/NCIC/III Manuals*

NCIC Operating Manual

NCIC Code Manual

III Manual

CJIS Security Policy

# Where to Find

# Questions?