BUREAU OF CRIMINAL IDENTIFICATION

BCI

DPS UTAH

INDUSTRY

UTAH

1847

1896

DEPARTMENT OF PUBLIC SAFETY

1927

How to Train Required Security Awareness Training

2018 TAC Conference

Outline

- Why is training required
- Levels
  - Who fits in each
  - What needs to be covered
- Tracking training
- Different approaches to training
- How to make training more effective

Notes from State Information Security Officer
Facts about Security Awareness

Why is Security Awareness Training (SAT) required?

Why SAT?

- To prevent and limit potential exposure to unintentional and intentional threats against the system
  - Natural threats
    - Disasters that could endanger facility or equipment
      - Fire
      - Flood
      - Lightning

Why SAT?

- To prevent and limit potential exposure to unintentional and intentional threats against the system
  - Natural threats
  - Unintentional threats
    - Actions that occur due to lack of knowledge or through carelessness
    - Can be prevented through awareness and training

Why SAT?

- To prevent and limit potential exposure to unintentional and intentional threats against the system
  - Natural threats
  - Unintentional threats
  - Intentional threats
    - Designed to deliberately harm or manipulate information systems, software or data

What about other Security Awareness Trainings?

HIPPA

Agency required SAT

Other Security Awareness Trainings

- Other trainings may be used to cover some topics
- But the training should focus on Security Awareness as it relates to CJIS data

  - Ex. Proper handling and marking of CJIS data.
    Encryption of CJIS data
    Incident response when CJIS data could have been compromised

What is CJIS Data?

- Any information provided by BCI via UCJIS to criminal justice agencies necessary for the administration of criminal justice.

- This data includes, but is not limited to:
  - Biometric
  - Biographic
  - Property
  - Case/incident
  - Motor vehicle
  - Driver license
  - Warrant
  - Protective order
  - Criminal history record

Security Awareness Fact #1

- What is the most expensive computer virus in history?

Levels of Security Awareness Training

Level One

Who

- All personnel with unescorted access to secured location
  - Janitors, repair men
- In BCI language
  - Non-users

What Needs to be Trained

- Responsibilities and expected behavior in regards to UCJIS information
- Implications of non-compliance
- Visitor control
- Physical access to spaces
- Incident response

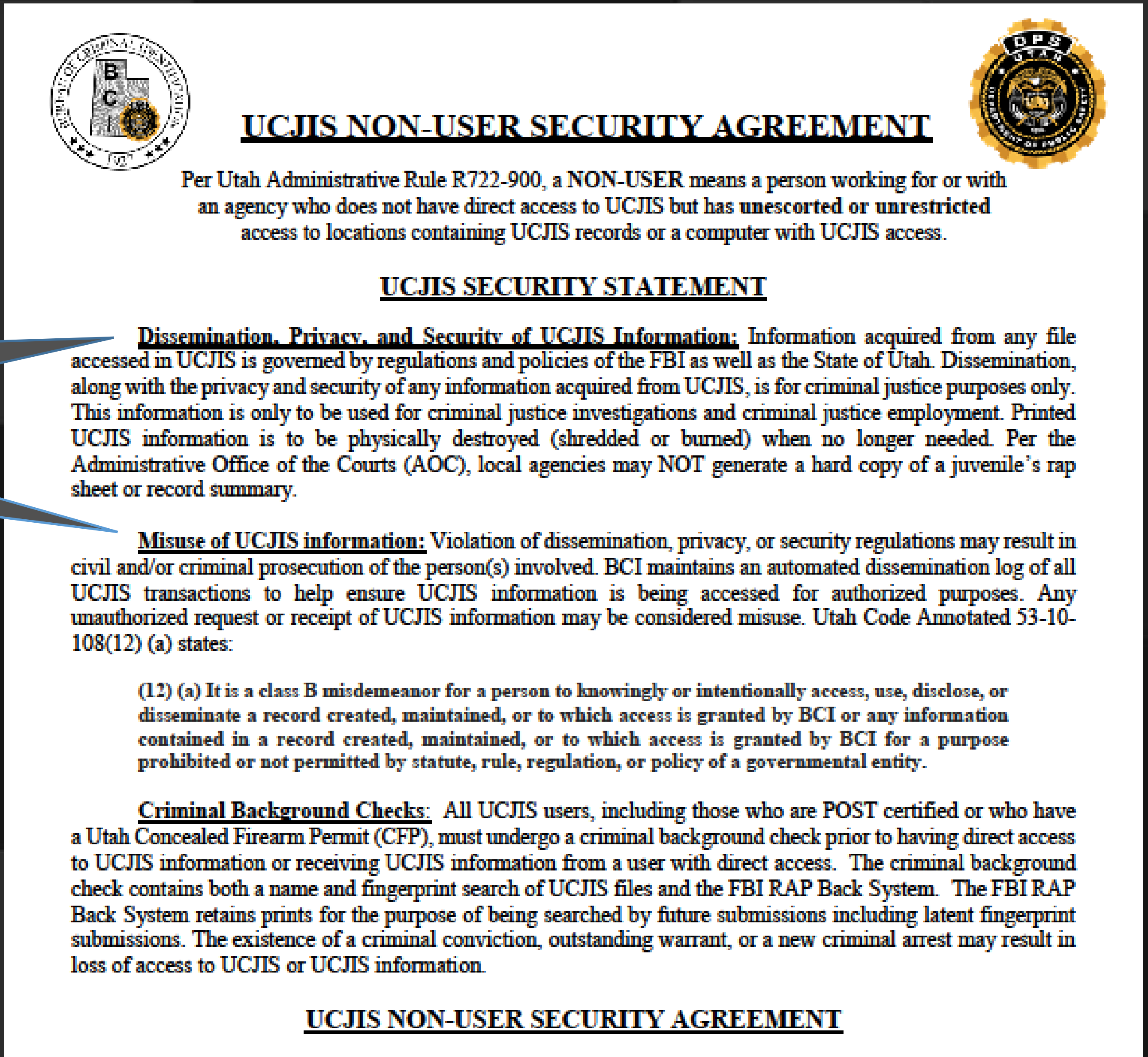
How?

- Non-User Security Agreement

Responsibilities and expected behavior

Implications of noncompliance

- Visitor Control and access to secure location
- What to do if there is an incident



UCJIS NON-USER SECURITY AGREEMENT

Per Utah Administrative Rule R722-900, a **NON-USER** means a person working for or with an agency who does not have direct access to UCJIS but has **unescorted or unrestricted** access to locations containing UCJIS records or a computer with UCJIS access.

UCJIS SECURITY STATEMENT

Dissemination, Privacy, and Security of UCJIS Information: Information acquired from any file accessed in UCJIS is governed by regulations and policies of the FBI as well as the State of Utah. Dissemination, along with the privacy and security of any information acquired from UCJIS, is for criminal justice purposes only. This information is only to be used for criminal justice investigations and criminal justice employment. Printed UCJIS information is to be physically destroyed (shredded or burned) when no longer needed. Per the Administrative Office of the Courts (AOC), local agencies may NOT generate a hard copy of a juvenile's rap sheet or record summary.

Misuse of UCJIS information: Violation of dissemination, privacy, or security regulations may result in civil and/or criminal prosecution of the person(s) involved. BCI maintains an automated dissemination log of all UCJIS transactions to help ensure UCJIS information is being accessed for authorized purposes. Any unauthorized request or receipt of UCJIS information may be considered misuse. Utah Code Annotated 53-10-108(12) (a) states:

> **(12) (a) It is a class B misdemeanor for a person to knowingly or intentionally access, use, disclose, or disseminate a record created, maintained, or to which access is granted by BCI or any information contained in a record created, maintained, or to which access is granted by BCI for a purpose prohibited or not permitted by statute, rule, regulation, or policy of a governmental entity.**

Criminal Background Checks: All UCJIS users, including those who are POST certified or who have a Utah Concealed Firearm Permit (CFP), must undergo a criminal background check prior to having direct access to UCJIS information or receiving UCJIS information from a user with direct access. The criminal background check contains both a name and fingerprint search of UCJIS files and the FBI RAP Back System. The FBI RAP Back System retains prints for the purpose of being searched by future submissions including latent fingerprint submissions. The existence of a criminal conviction, outstanding warrant, or a new criminal arrest may result in loss of access to UCJIS or UCJIS information.

UCJIS NON-USER SECURITY AGREEMENT

What Types of Security Incidents Need to be Reported to State Information Security Officer?

Reportable Incidents

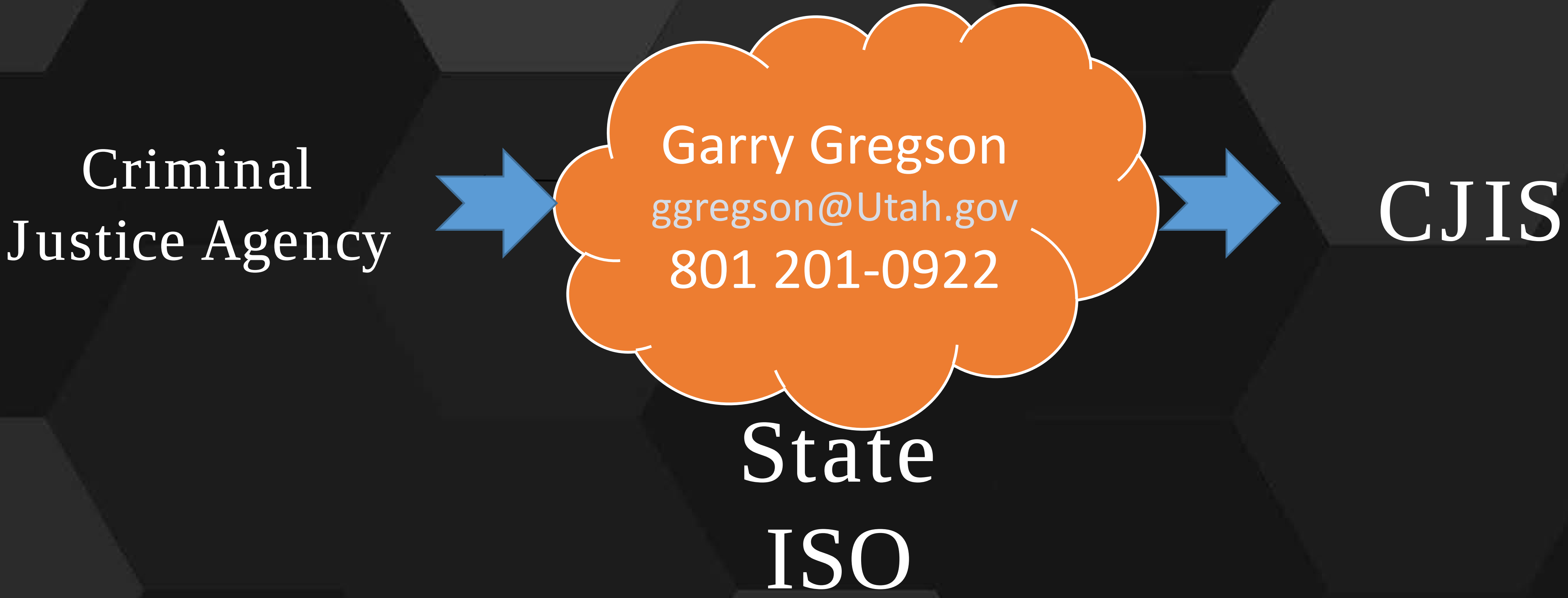
- Server containing CJIS data was hacked
- Denial of service
- Root/administrator compromise
- Virus infections where it is shown that CJIS data could have been compromised
- Unauthorized changes to hardware of software

Reportable Incidents

- Server containing CJIS data was hacked
- Denial of service
- Root/administrator compromise
- Virus infections where it is shown that CJIS data could have been compromised
- Unauthorized changes to hardware of software
- CJIS data leaked outside of a controlled area when proper handling procedures were not followed.
- Sending CJIS data unencrypted via email
- Unauthorized access of CJIS data

- Anything that could have or has compromised CJIS data in any fashion

Reporting Incidents



Criminal Justice Agency

Garry Gregson

ggregson@Utah.gov

801 201-0922

State ISO

CJIS

Level Two

Who

- All personnel with access to CJIS data (without a login)

- In BCI language
  - Non-access user

What Needs to be Trained

- All of level 1
- Protect information subject to confidentiality concerns
- Proper handling of CJIS data
  - Dissemination
  - Destruction
- Media protection
- Threats, vulnerabilities, and risks associated with handling of CJIS data
  - Social engineering

Level Three

Who

- All authorized personnel with both physical and logical access to CJIS data
  - **Physical**: Any kind of unescorted access within the secure perimeter of the agency, to wiring or equipment that accesses, processes, transmits or prints unencrypted CJIS data
  - **Logical:** Credentialed access (ie UserID and password) to a computer, network, applications or any other device or system that accesses, transmits or prints unencrypted CJIS data from outside the perimeter of the physically secure area of the entity

Who

- In BCI language
  - Users

What Needs to be Trained?

- All of level 1 and 2
- General rules that outline the responsibilities and behavior related to usage of information systems
- Creation, usage and management of passwords
- Web Usage – monitoring of user activity and prohibited sites
- Spam
- Specifics related to unknown attachments/emails
- Physical security- risks related to systems and data
- Protection that needs to be made with respect to Trojans, virus, malicious codes and malware
- Use of encryption techniques for transferring sensitive information over the Internet
- Issues related to access control
- Both information related and physical security with respect to laptops and their usage
- Issues associated with handheld devices and desktops as well
- Individual accountability including an explanation of what it means to the agency
- Specifics about if personally owned equipment is allowed by the agency or the state
- Specifics related to information security and confidential items, their usage, backup, archiving or destruction after its need is over.

Level Four

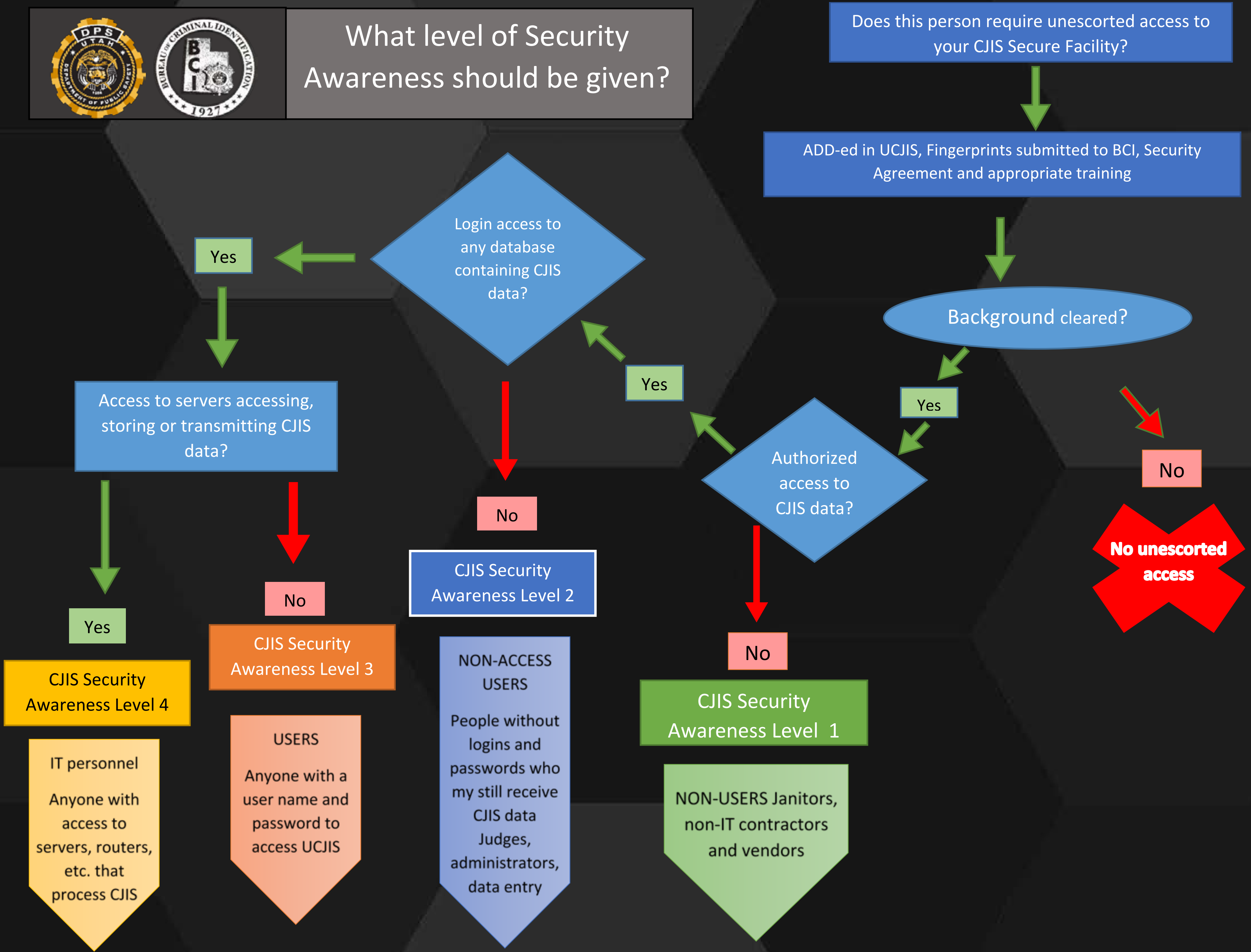
Who

- Personnel with an IT role

What Needs to be Trained

- All of level 1, 2, and 3
- Measures were taken for the protection of network infrastructure
- Access control measures
- Backup and storage of data and if the approach is centralized or decentralized
- Protection of the system and information from Trojans, worms, and viruses including scanning and updating of virus definitions
- As part of the configuration management, application and system patches need to be applied

What level of Security Awareness should be given?



Does this person require unescorted access to your CJIS Secure Facility?

ADD-ed in UCJIS, Fingerprints submitted to BCI, Security Agreement and appropriate training

Background cleared?

No

No unescorted access

Yes

Authorized access to CJIS data?

No

CJIS Security Awareness Level 1

NON-USERS Janitors, non-IT contractors and vendors

Yes

Login access to any database containing CJIS data?

No

CJIS Security Awareness Level 2

NON-ACCESS USERS

People without logins and passwords who my still receive CJIS data Judges, administrators, data entry

Yes

Access to servers accessing, storing or transmitting CJIS data?

No

CJIS Security Awareness Level 3

USERS

Anyone with a user name and password to access UCJIS

Yes

CJIS Security Awareness Level 4

IT personnel

Anyone with access to servers, routers, etc. that process CJIS

Security Awareness Fact #2

- How long would it take to crack your password?

Password Criteria (8 characters)	**Possible Combinations**
Lowercase alphabet	208,827,064,576
Upper and lowercase alphabet	53,459,728,531,456
Upper and lowercase alpha + numbers	218,340,105,584,896
Full set of allowed printable characters set	645,753,531,245,761

Security Awareness Fact #2

- How long would it take to crack your password?

Password Criteria (8 characters)	Possible Combinations	How long would it take on an average computer?
Lowercase alphabet	208,827,064,576	
Upper and lowercase alphabet	53,459,728,531,456	
Upper and lowercase alpha + numbers	218,340,105,584,896	
Full set of allowed printable characters set	645,753,531,245,761	

Security Awareness Fact #2

- How long would it take to crack your password?

Password Criteria (8 characters)	Possible Combinations	How long would it take on an average computer?
Lowercase alphabet	208,827,064,576	2 days
Upper and lowercase alphabet	53,459,728,531,456	1.44 years
Upper and lowercase alpha + numbers	218,340,105,584,896	5.88 years
Full set of allowed printable characters set	645,753,531,245,761	45.2 years

Security Awareness Fact #2

- How long would it take to crack your password?

Password Criteria (8 characters)	Possible Combinations	How long would it take on an average computer?	How long would it take on a supercomputer?
Lowercase alphabet	208,827,064,576	2 days	
Upper and lowercase alphabet	53,459,728,531,456	1.44 years	
Upper and lowercase alpha + numbers	218,340,105,584,896	5.88 years	
Full set of allowed printable characters set	645,753,531,245,761	45.2 years	

Security Awareness Fact #2

- How long would it take to crack your password?

Password Criteria (8 characters)	Possible Combinations	How long would it take on an average computer?	How long would it take on a supercomputer?
Lowercase alphabet	208,827,064,576	2 days	1.8 seconds
Upper and lowercase alphabet	53,459,728,531,456	1.44 years	7.6 minutes
Upper and lowercase alpha + numbers	218,340,105,584,896	5.88 years	31 minutes
Full set of allowed printable characters set	645,753,531,245,761	45.2 years	4 hours

Tracking of SAT

Tracking

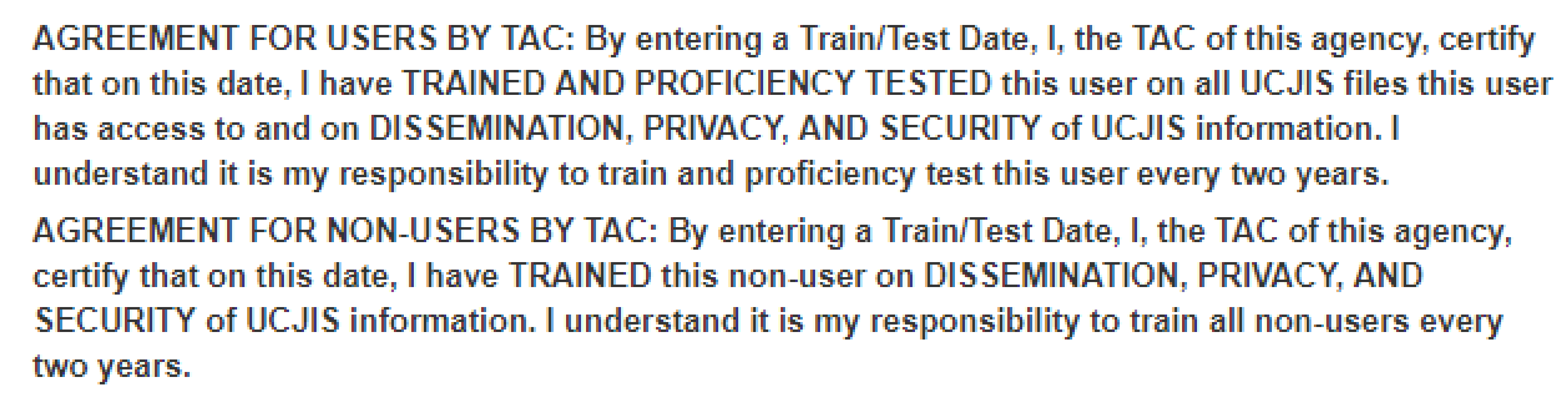
“Records of individual basic security awareness training and specific information system security training shall be documented, kept current, and maintained”

CJIS Security Policy 5.2.2

Tracking

How?

- Use CERT



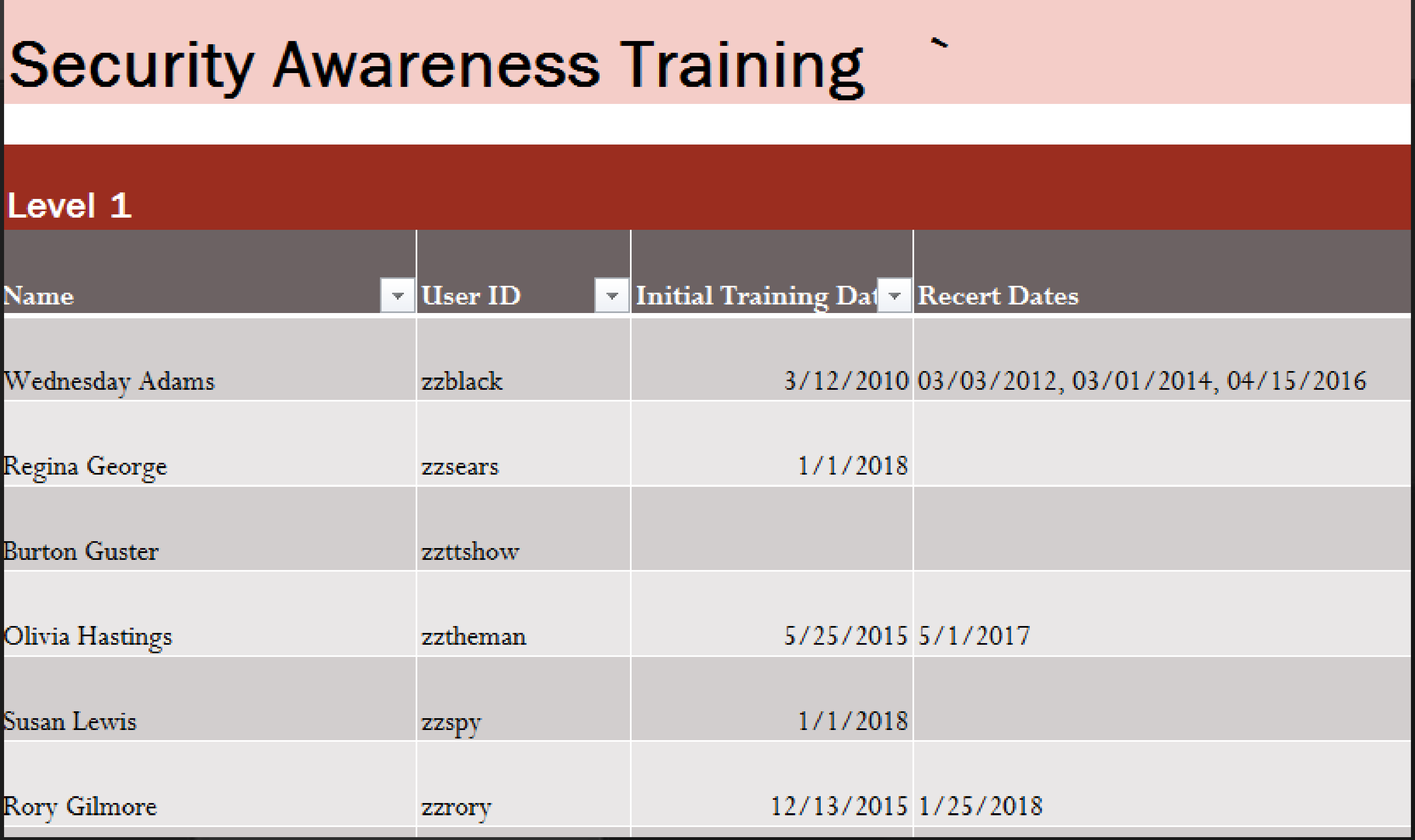
AGREEMENT FOR USERS BY TAC: By entering a Train/Test Date, I, the TAC of this agency, certify that on this date, I have TRAINED AND PROFICIENCY TESTED this user on all UCJIS files this user has access to and on DISSEMINATION, PRIVACY, AND SECURITY of UCJIS information. I understand it is my responsibility to train and proficiency test this user every two years.

AGREEMENT FOR NON-USERS BY TAC: By entering a Train/Test Date, I, the TAC of this agency, certify that on this date, I have TRAINED this non-user on DISSEMINATION, PRIVACY, AND SECURITY of UCJIS information. I understand it is my responsibility to train all non-users every two years.

Tracking

How?

- Use CERT
- Spreadsheet



Security Awareness Training `

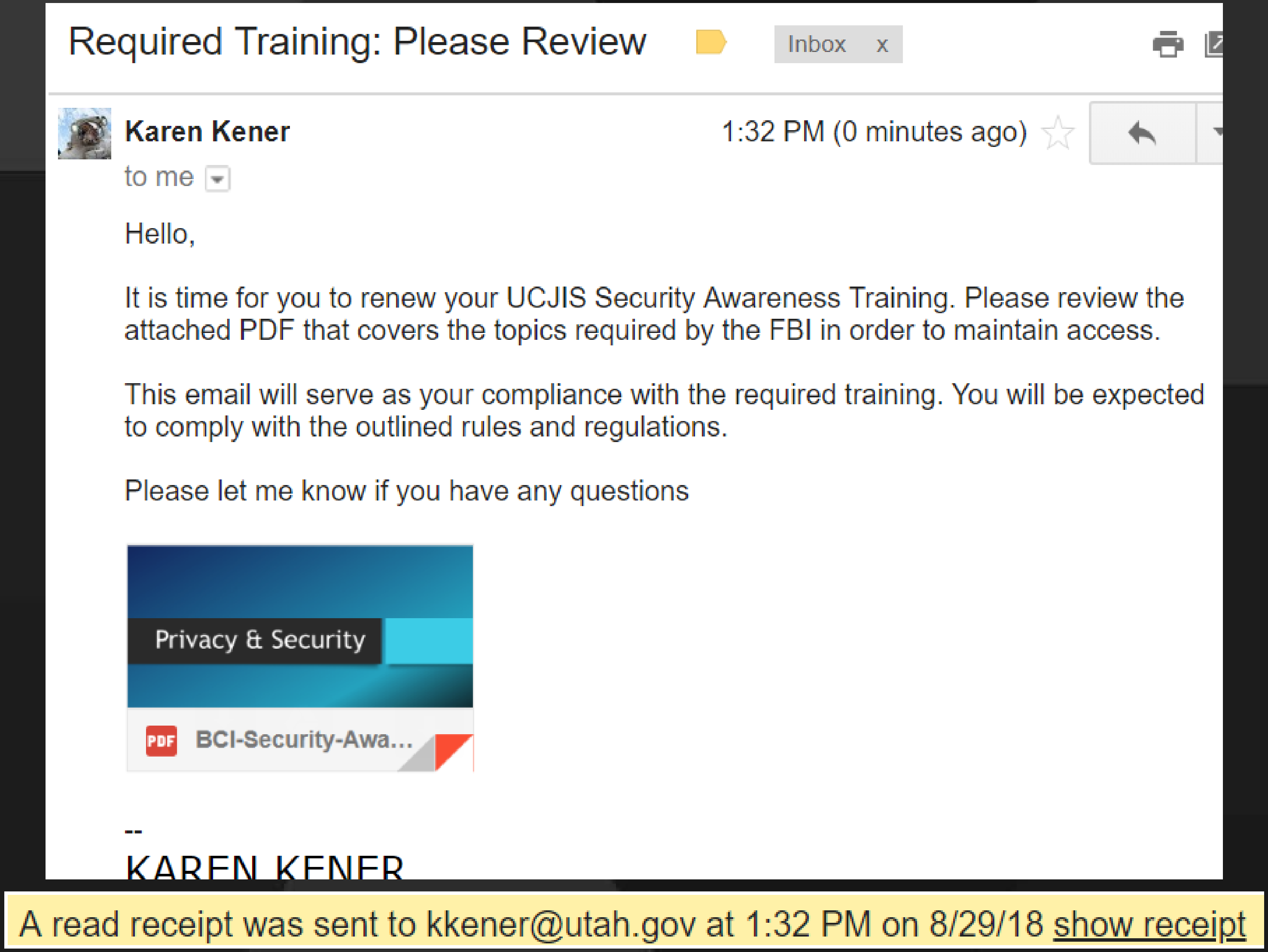
Level 1

Name	User ID	Initial Training Dat	Recert Dates
Wednesday Adams	zzblack	3/12/2010	03/03/2012, 03/01/2014, 04/15/2016
Regina George	zzsears	1/1/2018	
Burton Guster	zzttshow		
Olivia Hastings	zztheman	5/25/2015	5/1/2017
Susan Lewis	zzspy	1/1/2018	
Rory Gilmore	zzrory	12/13/2015	1/25/2018

Tracking

How?

- Use CERT
- Spreadsheet
- Read receipt



Required Training: Please Review

Karen Kener

to me

1:32 PM (0 minutes ago)

Hello,

It is time for you to renew your UCJIS Security Awareness Training. Please review the attached PDF that covers the topics required by the FBI in order to maintain access.

This email will serve as your compliance with the required training. You will be expected to comply with the outlined rules and regulations.

Please let me know if you have any questions

--

KAREN KENER

A read receipt was sent to kkener@utah.gov at 1:32 PM on 8/29/18 show receipt

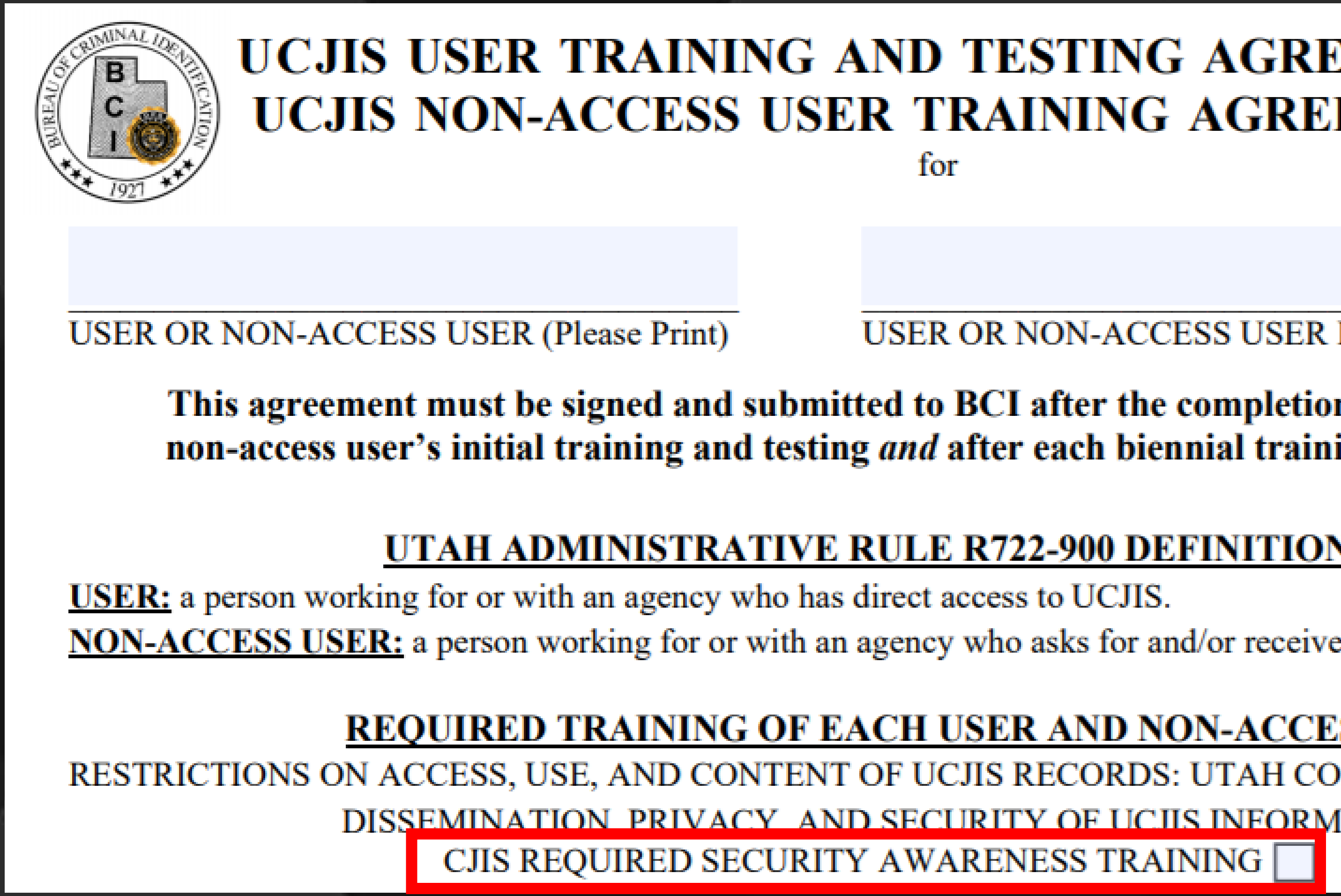
Security Awareness Fact #3

- In 2016, 95% of breached records come from what three industries?
  - Government
  - Retail
  - Technology

How to Train SAT

How to Train?

- Biennial training with user
  - User Training and Testing Agreement
  - TAC could require review of BCI's Security Awareness Power Point



UCJIS USER TRAINING AND TESTING AGRE

UCJIS NON-ACCESS USER TRAINING AGREI

for

USER OR NON-ACCESS USER (Please Print)

USER OR NON-ACCESS USER I

This agreement must be signed and submitted to BCI after the completion non-access user's initial training and testing *and* after each biennial traini

UTAH ADMINISTRATIVE RULE R722-900 DEFINITION

USER: a person working for or with an agency who has direct access to UCJIS.

NON-ACCESS USER: a person working for or with an agency who asks for and/or receive

REQUIRED TRAINING OF EACH USER AND NON-ACCE

RESTRICTIONS ON ACCESS, USE, AND CONTENT OF UCJIS RECORDS: UTAH CO

DISSEMINATION, PRIVACY, AND SECURITY OF UCJIS INFORM

CJIS REQUIRED SECURITY AWARENESS TRAINING □

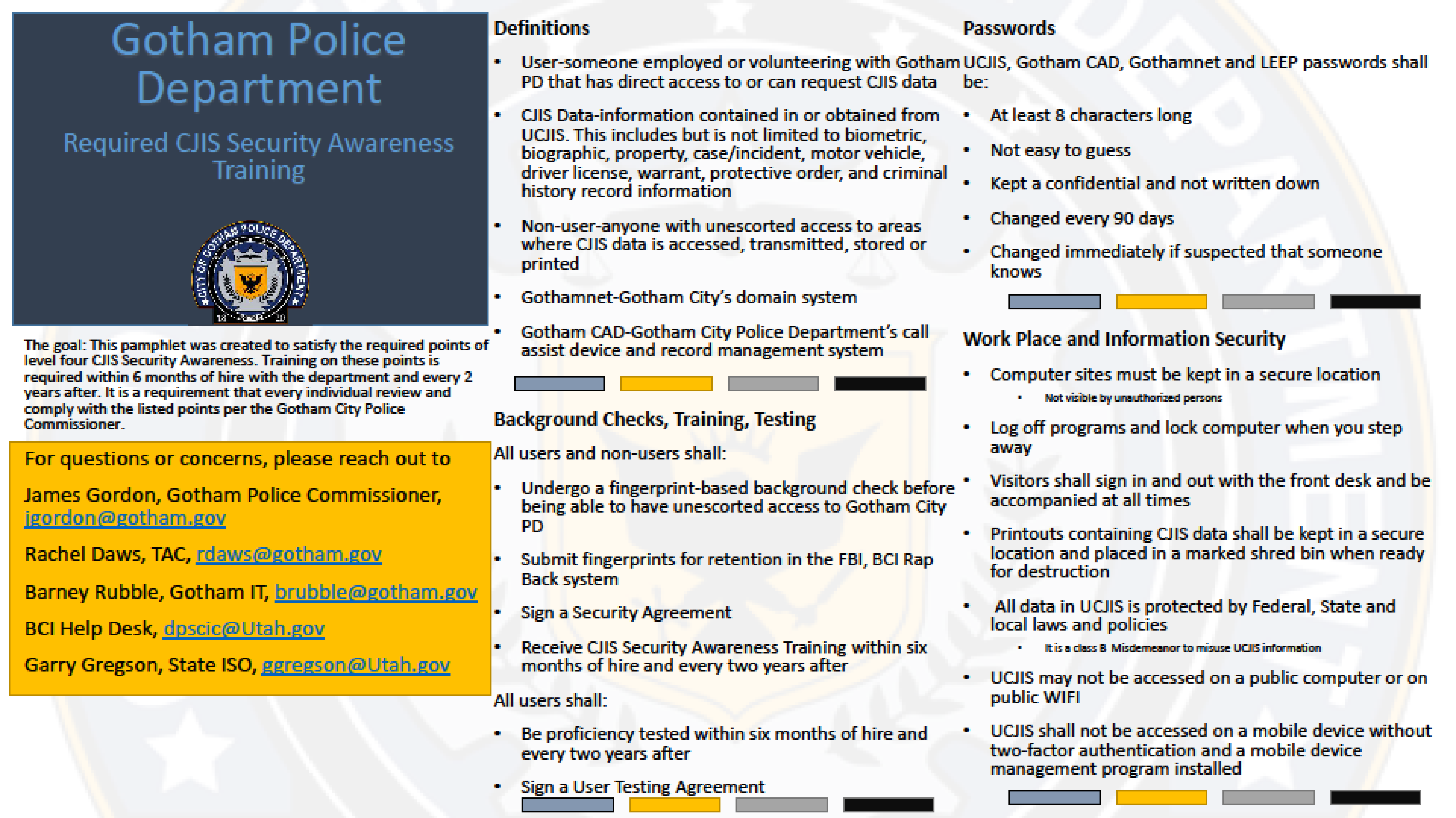
How to Train?

- Self review
  - Provide BCI presentation

Privacy & Security

How to Train?

- Self review
  - Provide BCI presentation
  - Create one-sheet



Gotham Police Department

Required CJIS Security Awareness Training

The goal: This pamphlet was created to satisfy the required points of level four CJIS Security Awareness. Training on these points is required within 6 months of hire with the department and every 2 years after. It is a requirement that every individual review and comply with the listed points per the Gotham City Police Commissioner.

For questions or concerns, please reach out to

James Gordon, Gotham Police Commissioner, jgordon@gotham.gov

Rachel Daws, TAC, rdaws@gotham.gov

Barney Rubble, Gotham IT, brubble@gotham.gov

BCI Help Desk, dpscic@Utah.gov

Garry Gregson, State ISO, ggregson@Utah.gov

Definitions

- User-someone employed or volunteering with Gotham PD that has direct access to or can request CJIS data
- CJIS Data-information contained in or obtained from UCJIS. This includes but is not limited to biometric, biographic, property, case/incident, motor vehicle, driver license, warrant, protective order, and criminal history record information
- Non-user-anyone with unescorted access to areas where CJIS data is accessed, transmitted, stored or printed
- Gothamnet-Gotham City's domain system
- Gotham CAD-Gotham City Police Department's call assist device and record management system

Background Checks, Training, Testing

All users and non-users shall:

- Undergo a fingerprint-based background check before being able to have unescorted access to Gotham City PD
- Submit fingerprints for retention in the FBI, BCI Rap Back system
- Sign a Security Agreement
- Receive CJIS Security Awareness Training within six months of hire and every two years after

All users shall:

- Be proficiency tested within six months of hire and every two years after
- Sign a User Testing Agreement

Passwords

UCJIS, Gotham CAD, Gothamnet and LEEP passwords shall be:

- At least 8 characters long
- Not easy to guess
- Kept a confidential and not written down
- Changed every 90 days
- Changed immediately if suspected that someone knows

Work Place and Information Security

- Computer sites must be kept in a secure location
  - Not visible by unauthorized persons
- Log off programs and lock computer when you step away
- Visitors shall sign in and out with the front desk and be accompanied at all times
- Printouts containing CJIS data shall be kept in a secure location and placed in a marked shred bin when ready for destruction
- All data in UCJIS is protected by Federal, State and local laws and policies
  - It is a class B Misdemeanor to misuse UCJIS information
- UCJIS may not be accessed on a public computer or on public WIFI
- UCJIS shall not be accessed on a mobile device without two-factor authentication and a mobile device management program installed

How to Train?

- Group review
  - All at once
    - Special time frame to focus on Security Awareness
      - Security Awareness Month
      - Security Awareness Week
      - 12 days of Security Awareness

On the twelfth day of security awareness training, my TAC reminded me:

- Not to trust unknown emails and attachments
- The consequences of misuse
- To change my password regularly
- Keep my training current
- Protect the information
- My fingers are in Rap Back
- Only access data for the administration of criminal justice
- Destroy or sanitize media
- Keep things secure
- Report security incidents
- Don’t ignore computer updates

How to Train?

- Group review
  - All at once
    - Biennial in-service with agency
      - Already mandatory and in place
      - Get yourself on the roster

• 2018 •

Officer In-Service

Mandatory

Utah Department of Public Safety

August-

10:00 AM-12:30 PM

BCI

How to Train?

- Group review
  - All at once
  - Continual training

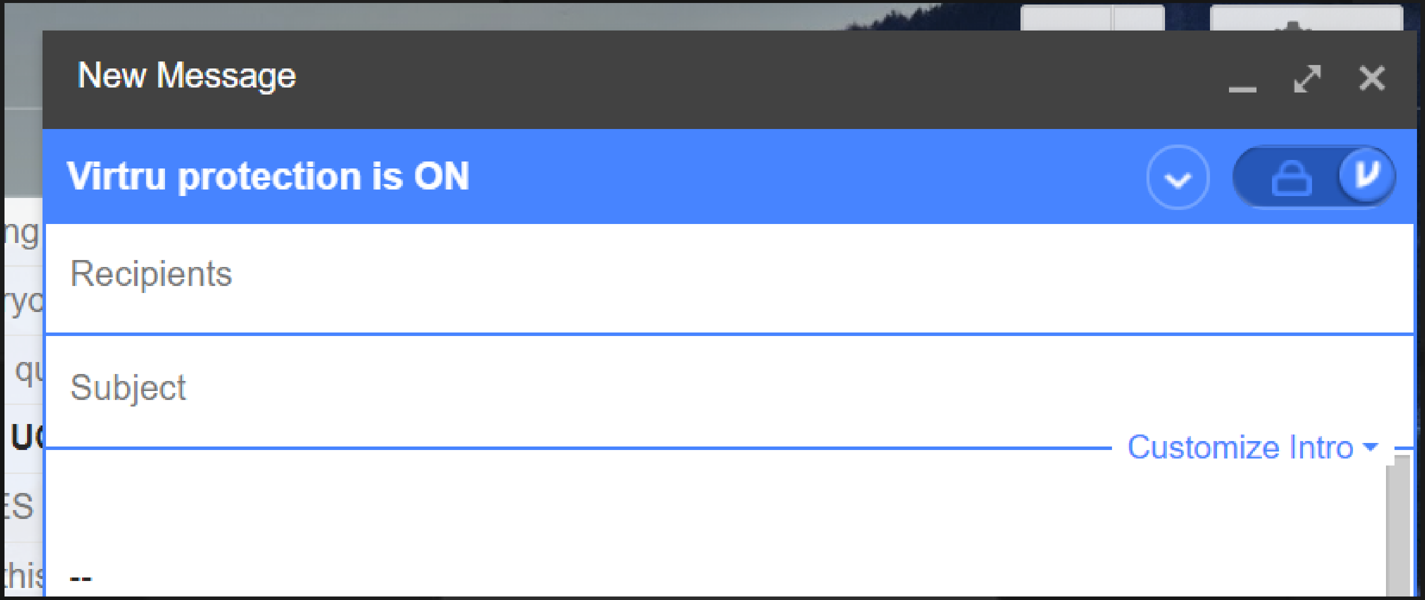
How to Train?

- Group review
  - Continual training
    - Staff meetings
      - Regularly occurring
      - Small, single factor thought
        - For users, 27 points that must be covered in 24 months

Encryption

- What needs to be encrypted?
  - Anything containing any CJIS data

- How do you encrypt?



New Message

Virtru protection is ON

Recipients

Subject

How to train?

- Group review
  - Continual training
    - Newsletters/Training email
    - Don’t have one?

      Start one

Gotham Police Department

NEWSLETTER

Volume 4

MEET THE NEW CHIEF

PASSWORD

- Avoid using perso information such birthdays, hobbi favorite sports tea names of fam friends or pets
- Try not to use dictionary word name

Making SAT More Effective

Tip for Making SAT More Effective

- Enlist support from the top
  - If the boss says it has to be done, it will likely be done

Tip for Making SAT More Effective

- Choose the right method
  - How much time do you have?
  - Will you be doing this alone?
  - What has/hasn’t worked in the past?

Tip for Making SAT More Effective

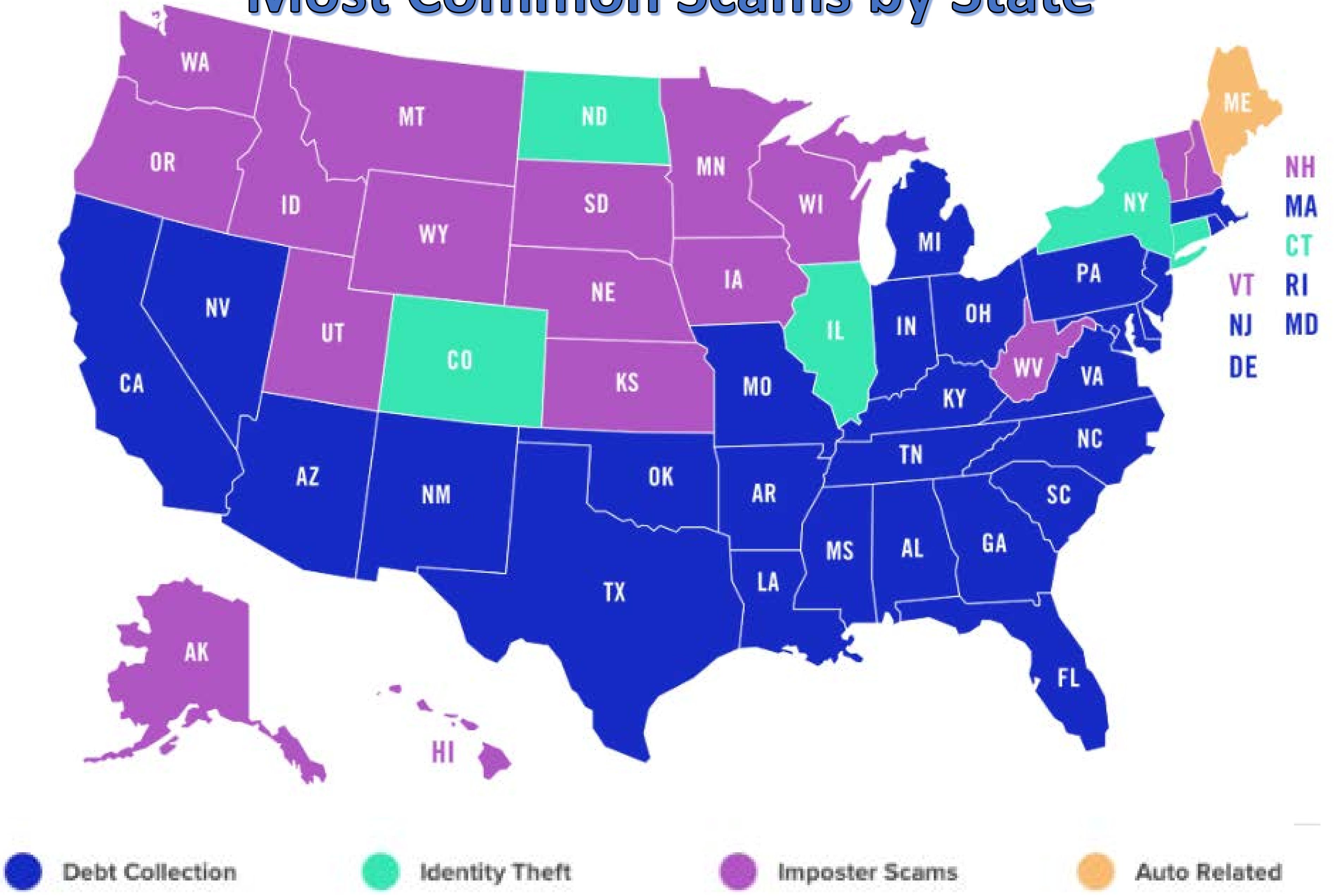
- Use real life social engineering examples
  - Partner with your IT
    - Are there any scams, phishing, hacking examples from our agency?
  - Find local examples
    - Google news stories in your area of on going or recent
    - Find agency related examples (Other PDs, courts, government bodies)

Tip for Making SAT More Effective

- Engage your audience
  - Ask the audience questions
    - How many of you use the same password for multiple accounts?
    - How many of your have received a scam email?
      - Ask for examples

Security Awareness Fact #4

Most Common Scams by State



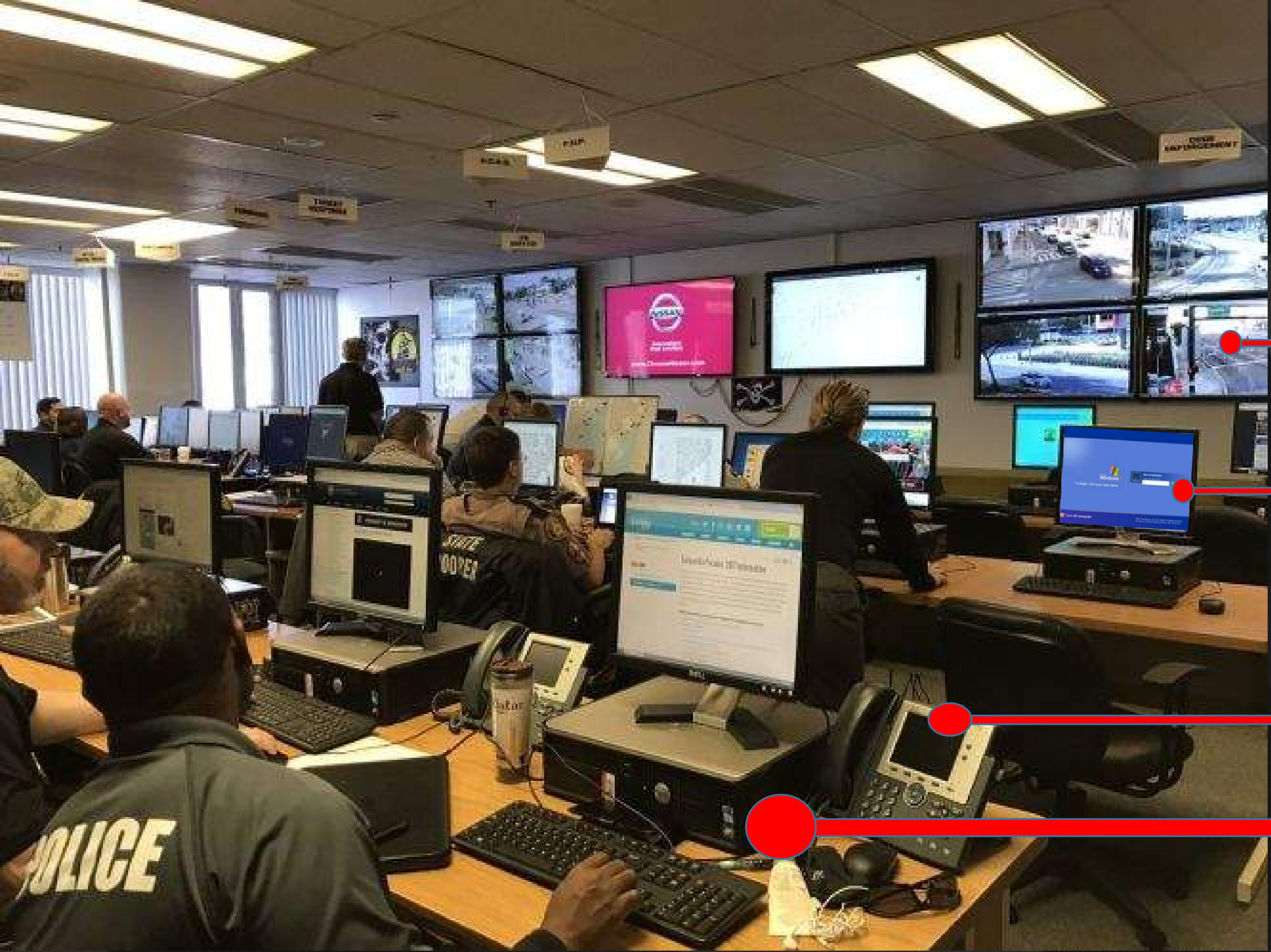
Tip for Making SAT More Effective

- Engage your audience
  - Have them think like a hacker
    - Google your agency
      - See what information is accessible and viewable about your agency
        - Are your contracts public?
        - Are your building floor plans available online?

Tip for Making SAT More Effective

- Engage your audience
  - Review your agencies social media presence
    - What do the pictures posted tell about your agency?
      - Entry credentials?
      - Technology used?
      - Work schedules?

CODE ENFORCEMENT
THREAT RESPONSE
POLICE



Camera placement

Operating system version

Phone system information

Desktop/laptop hardware

Security Awareness Fact #5

- What is the primary risk factor for successful cyberattacks?
  - Human error
  - 95% of successful cyberattacks are the result of a phishing scam
  - Successful awareness training can reduce risk by up to 70%

How does your agency approach Security Awareness Training?

BUREAU OF CRIMINAL IDENTIFICATION

BCI

1927

DPS

UTAH

INDUSTRY

UTAH

1896

DEPARTMENT OF PUBLIC SAFETY