

Welcome to FBI CJIS Policy Security Awareness Training



Navigating the Course - Table of Contents (TOC)

To the right is an example of the Table of Contents Bar (TOC). This bar can be used as a navigation tool.

To open the TOC, simply click on the TOC button on the navigation bar.



The TOC will display over the course on the left side. To navigate to a specific slide, simply click on the slide you wish to visit. To collapse the TOC, either click on the TOC button on the navigation bar or click the collapse button found on the right side of the TOC

Table Of Contents	
<input checked="" type="checkbox"/>	Slide Title
<input type="checkbox"/>	Slide 3
<input type="checkbox"/>	Slide 3
<input type="checkbox"/>	Slide 4



This course outlines the policies and procedures each employee and agency must follow in order to maintain compliance with the FBI Criminal Justice Information Services (CJIS) Security Policy.

The CJIS Security Policy provides minimum security requirements associated with creation, viewing, modification, transmission, dissemination, storage, or destruction of Criminal Justice Information (CJI). Your agency may have further policies and procedures in addition to CJIS policy. Those policies may be more strict than FBI CJIS.



Click the forward button to continue.

Helpful Hints

- Useful Resources
 - CJIN User's Guide (CUG)
 - FBI CJIS Security Policy Version 5.7
- This course does not require CJIN Access
- This course requires Adobe Acrobat Reader to open PDF documents
- This course should function on all modern browsers



Click the forward button to continue.

Criminal Justice Information is data on people, vehicles, and property accessed in the performance of official “criminal justice duties.” In other words, data you need to do your job. This includes vehicle registration and drivers’ license records, drivers’ license photos, criminal history records, CJIN and NCIC hits on wanted persons, stolen vehicles, stolen property, etc... Basically, if you access information through CJIN, it is CJI.

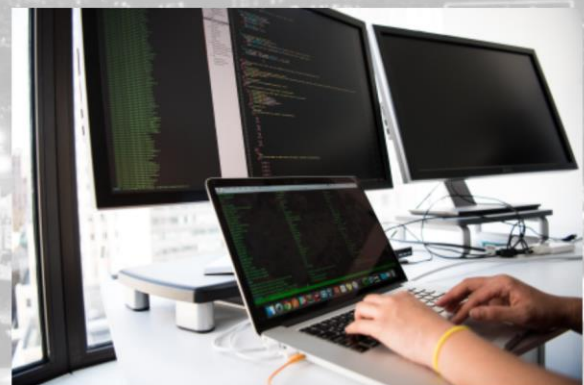
Criminal Justice Information is confidential and highly protected. It is only to be used for criminal justice and public safety purposes. Click on the photo to learn more about what CJI is.



Click the forward button to continue.

Security Awareness Training is mandatory for all personnel who have access to Criminal Justice Information in any form. This includes reading, writing, processing, or transmitting, as well as, unescorted access to a physically secure area.

- Must be completed within 6 months of hire and
- Every 2 years after initial completion



Who is considered having unescorted access?

Click the box above to learn more about unescorted access.

Click the forward button to continue.

Mandatory Training

Security Awareness Training is mandatory for anyone who has access to any of the following processes or unescorted access to a secure area.

Unescorted Access is a term given to anyone who does not directly handle Criminal Justice Information but is granted access to secure areas where Criminal Justice Information may be present.

Example: janitorial staff, private contractors (painters, maintenance, phone/internet providers)

- Must
- of
- Every

Click to Close

Who is considered having unescorted access?

Click the box above to learn more about unescorted access.

Click the forward button to continue.

Personnel Access

Prior to granting unescorted access to a secure location or access to Criminal Justice Information, both fingerprint-based and name-based background checks are required to be submitted to the state by the hiring agency. The results of the background check must be kept on file within your agency.

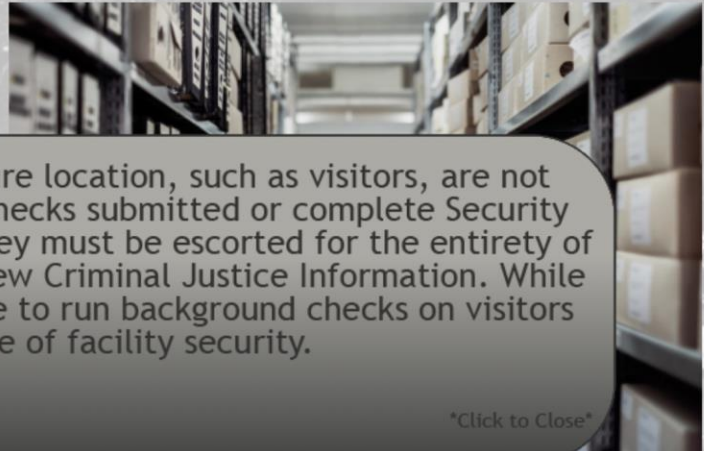


Escorted Access

Click the box above to learn about escorted access.

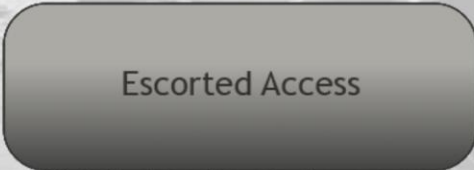
Click the forward button to continue.

Prior to granting unescorted access to a secure location or access to Criminal Justice



Anyone escorted inside a secure location, such as visitors, are not required to have background checks submitted or complete Security Awareness Training. However, they must be escorted for the entirety of their visit and not allowed to view Criminal Justice Information. While not required, it is good practice to run background checks on visitors for the purpose of facility security.

Click to Close



Click the box above to learn about escorted access.

Click the forward button to continue.

All secure areas must be clearly marked with an “Authorized Personnel Only” sign. Notify your supervisor if there is not a sign posted restricting access to an area that contains Criminal Justice Information.

All visitors’ identities must be verified before granting access to secure locations. Visitors must be monitored when entering and exiting secure areas and accompanied at all times. It is suggested to have a visitor log to ensure documentation of who is in the building at any given time.



Click the forward button to continue.

You are in your facility everyday and know your surroundings better than anyone. If you see a suspicious person or activity, say something.

Immediately notify your Terminal Agency Coordinator (TAC) or supervisor of any possible security threat. Any form of security breach should be reported to DOJ IT department by your supervisor. If your supervisor or TAC is not available, follow your agency's policies and procedures.



Click on the picture to learn about threats to your agency



Click on JITSD's logo for their contact info

Click the forward button to continue.

You are in your facility everyday and know your surroundings better than anyone. If you see a suspicious person or activity, say something.

Immediately notify your Terminal Agency Coordinator (TAC) or supervisor of any possible security threat. Any form of security breach should be reported to DOJ IT department by your supervisor. If your supervisor or TAC is not available, follow your agency's policies and procedures.



Click on the picture to learn about threats to your agency

- Examples of possible threats:
- Unauthorized personnel attempting to enter a secure area
 - Impersonating an officer or other employee to gain information or access to a secure area
 - Someone taking photos of CJJ on their cell phone or other device
 - Eliciting information about an event or subject outside of their job description
 - CJJ printouts found on the floor or outside of secure area

Click to Close



Click on JITSD's logo for their contact info

Click the forward button to continue.

Responsibility

Montana's law enforcement personnel are held to a high standard of public respect. Following FBI and local policies to preserve the confidentiality of Criminal Justice Information is crucial in maintaining this respect. Whether you are in the vicinity of Criminal Justice Information, receive the printouts, or transmit the queries yourself, you are expected to secure the information and not expose it to threats.

It is your responsibility to protect Criminal Justice Information and ensure it is only being used for criminal justice or public safety purposes. Always be aware of your surroundings!

If you suspect someone abusing Criminal Justice Information or not using it for its intended purpose, report it to your TAC or supervisor immediately.

Click the forward button to continue.

Noncompliance

There are serious consequences for misusing Criminal Justice Information and exposing state and federal systems to threats:

- ◆ Violating public trust
- ◆ Loss of credibility and respect for yourself and other members of the law enforcement community
- ◆ Termination of access
- ◆ Termination of employment
- ◆ Criminal prosecution (See 45-7-601 MCA)
- ◆ Civil liability



Click the forward button to continue.

Multiple Choice

You notice someone that you know is not an employee lurking around the Sheriff's office and peering in windows right before you leave for break. What should you do?

- A) Immediately document this person in your suspicious person activity log
- B) Immediately report this person to your TAC or supervisor
- C) Go to lunch and see if they are still there when you return
- D) Do nothing, there are always people around the Sheriff's office

Question 1 of 25

Multiple Choice

Select everyone who must have fingerprint and name based background checks submitted and enroll in Security Awareness Training before being allowed access to a restricted area where CJI is present.

- A) The facility's janitor who will be unescorted
- B) The Police Chief's spouse visiting for lunch and will be escorted
- C) The Terminal Agency Coordinator
- D) The recently hired dispatcher

Question 2 of 25

Multiple Choice

How often is Security Awareness Training required by the FBI to be completed?

- A) Within the first 6 months and then biennially after that
- B) Within the first 6 months and then annually after that
- C) Monthly, in case of any updates
- D) Only one time when the person is hired

Question 3 of 25

Submit

Multiple Choice

You find a printout containing CJI on an empty desk outside of the secure area of your building. What should you do with it?

- A) Keep it in case someone is looking for it
- B) Leave it where you found it because someone will come back for it
- C) Immediately take it to your TAC or supervisor
- D) Put it inside the desk so it is not out in the open

Question 4 of 25

Submit

Multiple Choice

You find a printout containing CJI on an empty desk outside of the secure area of your building. What should you do with it?

- A) Keep it in case someone is looking for it
- B) Leave it where you found it because someone will come back for it
- C) Immediately take it to your TAC or supervisor
- D) Put it inside the desk so it is not out in the open

Question 4 of 25

True/False

As long as a visitor signs in to the visitation log, they are free to roam all areas of the building including the secure areas because their visit is documented.

- A) True
- B) False

Question 5 of 25

Media Protection



All CJI photos, documents and other media must be protected whether in digital or physical format and stored within physically secure locations. You and your agency must establish safeguards to ensure the security and confidentiality of the information.



Click each object to learn more about media



**** ALWAYS** establish that the person you are sending or giving CJI to is authorized to receive the information!**

Click the forward button to continue.

Media Protection



Do not leave USB Flash Drives, CDs, hard drives, or other digital media storage devices containing Criminal Justice Information where the public can potentially have access to them.

Click to Close



Click each object to learn more about media



**** ALWAYS** establish that the person you are sending or giving CJI to is authorized to receive the information!**

Click the forward button to continue.

Media Protection

Physical documents containing CJI should never be in public view such as by windows or on desks accessible to the public. If transporting physical documents, ensure they are hidden from view in a folder or envelope during transport and only given to authorized individuals. *Click to Close*



Click each object to learn more about media



**** ALWAYS** establish that the person you are sending or giving CJI to is authorized to receive the information!**

Click the forward button to continue.

Media Protection

NEVER leave undocked mobile terminals unattended, especially in a public place such as a restaurant or cafe. *Click to Close*



Click each object to learn more about media



**** ALWAYS** establish that the person you are sending or giving CJI to is authorized to receive the information!**

Click the forward button to continue.

Media Protection

Always encrypt Criminal Justice Information sent electronically before sharing with another agency or putting it on a device that could be lost or stolen such as a USB drive. This means you cannot send CJI through your email unless your email is encrypted. Faxes sent over a telephone line are exempt from the encryption requirement, however, the fax must be in a secure area and the recipient must be authorized to receive the information.

Click to Close



Click each object to learn more about media



**** ALWAYS** establish that the person you are sending or giving CJI to is authorized to receive the information!**

Click the forward button to continue.

Social Media

Social media can be a helpful investigative resource for law enforcement when used correctly. However, there are strict regulations for posting on social media and other online forums.

- Photos, videos, or links containing CJI are protected and shall not be displayed on the internet
- CJI printouts or any documents containing personally identifiable information (PII) should never be uploaded

Click on the Facebook logo to see social media exceptions

facebook



YouTube

Click the forward button to continue.

ONLY a person's driver's license photo can be uploaded to social media if:

- they are a wanted person with a warrant on file
- they are a missing person with a missing person report

(This does NOT mean their entire driver's license return can be uploaded. ONLY the DL photo can be used under these circumstances.)

Click to Close

Click on the Facebook logo to see social media exceptions

facebook



Click the forward button to continue.

Select the circumstances in which you are allowed to upload a person's drivers license photo to social media.

- A) They are a wanted person with a warrant on file
- B) You are never allowed to post a drivers license photo on the internet
- C) They are a missing person with a missing person report on file
- D) They are a person of interest in a bank robbery

Question 6 of 25

Submit

True/False

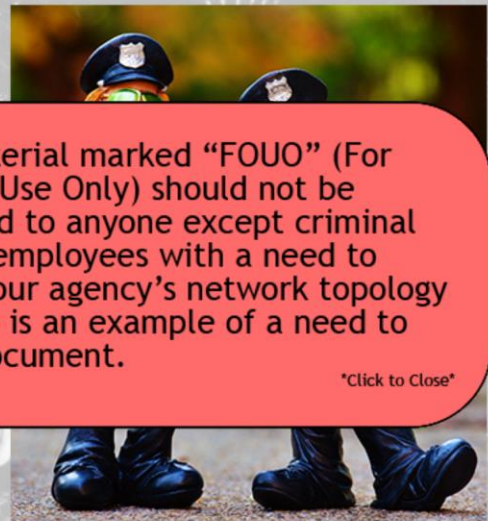
Faxes sent over a telephone line in a secure area to a recipient that is authorized to receive the information are exempt from requiring encryption.

- A) True
- B) False

Question 7 of 25

Handling and Marking CJJ

All CJJ should be clearly labeled and kept in a physically secure area. This includes CJJ printouts, any storage devices that contain CJJ, and CJIN terminals.



Information that has been extracted and entered into CAD or RMS systems is still Criminal Justice Information and requires protection.

Click to Close

Any material marked "FOUO" (For Official Use Only) should not be disclosed to anyone except criminal justice employees with a need to know. Your agency's network topology diagram is an example of a need to know document.

Click to Close

CAD Systems

FOUO

Click the forward button to continue.

! DANGER

- Internal threats- vulnerabilities people within your agency create
- ◆ Snooping for non-work related information
 - ◆ Telling friends and family confidential work information
 - ◆ Sharing information with the press or other organizations
 - ◆ Stealing paperwork or USB drives
 - ◆ Deliberately destroying or deleting information

! DANGER

- External threats- vulnerabilities outside your agency
- ◆ Physically accessing secure areas where CJIS is present
 - ◆ Email and phone scams
 - ◆ Viruses and other malicious malware
 - ◆ Hackers
 - ◆ Members of the public viewing CJIS purposefully or accidentally



Click the forward button to continue.

As mentioned previously, Criminal Justice Information is only for criminal justice and public safety purposes. Someone engaged in social engineering poses a threat to CJIS security. The reason this is so dangerous is because the victim rarely comes face-to-face with the attacker. It is done online or over the phone and often leads to the criminal gaining access to the victim's computer system and confidential information. The digital contact makes it easy for the attacker to disguise themselves.

Social engineering occurs when someone uses deception to manipulate a victim into performing actions or divulging confidential information.



[Click here to see an example of social engineering](#)

Click the forward button to continue.

Social Engineering

Always verify who you are speaking with whether in person, on the phone, or via email before sharing information. An easy method for doing this is asking for their contact information so you can call them back. Instead, call their employer and verify their employment. You should also ask for their credentials if they are in person or for their ORI when on the phone.

Common types of social engineering:

1. Phishing-seeks to obtain personal info using link shorteners or embedded links that redirect users to suspicious websites
2. Pretexting-focused on creating a fabricated scenario to build a false sense of trust with their victim to elicit information
3. Tailgating- also called “piggybacking” occurs when someone unauthorized follows an employee into a restricted area or uses their credentials to access websites or data bases

Phishing

Pretexting

Tailgating

Click each of the boxes above for examples of each type of social engineering.



Click the forward button to continue.

Social Engineering

Your agency uses Amazon to order some of the tactical gear for its officers. You receive an email from Amazon saying there is an issue with your account and you need to use your log-in info to update your account. However, the link will take you to an unknown website.

You receive a call from an unknown number. The person on the line says to you, “Hello, I am Detective Jones. Can you please send me criminal history on James Smith?” Without verifying his identity first, you could be victim to pretexting and compromising your agency.

Someone impersonating a delivery driver is waiting outside holding a box when you get to work. Once you gain access to the secure building, he asks you to hold the door and follows you inside.

Click to Close

Phishing

Pretexting

Tailgating

Click each of the boxes above for examples of each type of social engineering.



Click the forward button to continue.



Steps to protect you and your agency from social engineering:

- ◆ Do not open emails from untrusted sources
- ◆ If an offer from a stranger seems too good to be true, it probably is
- ◆ Lock your computer or mobile terminal when not present
- ◆ Ensure anti-virus software is up to date
- ◆ Know your agencies policies and procedures
- ◆ If you see something, say something

Click the forward button to continue.

Dissemination is the communication or transfer of Criminal Justice Information. Sharing CJI is one of law enforcement's greatest tools, but policies are in place to guarantee the protection of confidential information.

Primary Dissemination-The person requesting the CJI is given the CJI over the radio, by printout, or fax.

Secondary Dissemination- The initial recipient passes the CJI to another authorized criminal justice professional. A secondary dissemination log must be written and maintained by the originating agency any time secondary dissemination occurs.

Click here for an acceptable primary dissemination example

Click here for an acceptable secondary dissemination example



Click the forward button to continue.

Dissemination

Dissemination is the communication or

An officer requests a criminal history check from their dispatch center. Once the query is transmitted, the information is handed to the officer at the jail.

Click to Close

Click here for an acceptable primary dissemination example

Primary Dissemination-The person requesting the CJJ is given the CJJ over the radio, by printout, or fax.

Click here for an acceptable secondary dissemination example

Your county attorney requests a copy of the criminal history before court. The officer then takes the copy they were given from their dispatcher, fills out the secondary dissemination log and faxes it to the county attorney.

Click to Close

dissemination occurs.



Click the forward button to continue.

Transmission Exercise

The right side of the screen has examples of typical documents you may send to other agencies. The left side has the two methods for sending documents. Click and drag each document from the right side to the authorized sending method on the left side of the screen. If you make a mistake, the "Undo" button will undo the last step you took. To start over completely, select the "Reset" button. Once you are pleased with your answers, select "Submit" to see how you did! Click anywhere on this screen to close this bubble and get started.

Click to Close

The interface shows a workspace with document thumbnails on the right and sending method icons on the left. The thumbnails include a blue 'EMAIL' icon, a 'MONTANA DRIVER LICENSE' card, a 'Memo' document, and a 'CRIMINAL HISTORY' document. The sending methods on the left are represented by a blue envelope icon labeled 'FAX' and a blue document icon labeled 'EMAIL'. At the bottom of the workspace are four buttons: 'Instructions', 'Undo', 'Reset', and 'Submit'.

Destruction

Once CJIS is no longer needed, it must be destroyed. Physical documents must be shredded or incinerated and digital files need to be overwritten.

Shredding must be done by a cross cut shredder or a vendor approved by the DOJ. If shredding is done by a third party vendor, it must take place on site with authorized agency personnel present.



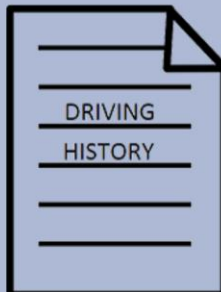
Keep the amount of documents waiting to be destroyed to a minimum. This means no excess of "to be shredded" piles.

Click the forward button to continue.

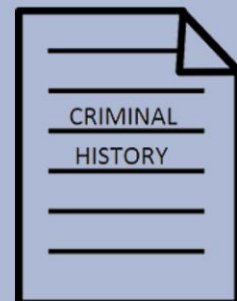
Transmission Exercise



Memo form with fields for To, From, Date, and Subject.



Court Notification form.



Transmission Exercise

Court Notification



Instructions

Submit

Multiple Choice

What is required if you provide CJ to an authorized agency outside your organization?

- A) It is never acceptable to give CJ to anyone outside of your agency
- B) Whenever the person or property has left the jurisdiction of the originating agency, CJ should be transferred to the agency with jurisdiction
- C) A secondary dissemination log is completed by the originating agency and includes the name of the intended recipient of the information
- D) CJ can be given to any other law enforcement agency if they request it as long as it is protected in transit

Question 8 of 25

Submit

Matching



Match the following types of social engineering to its corresponding example

Social Engineering Type

- Phishing
- Pretexting
- Tailgating
- Social Engineering

A) Example

- A) A caller tries to gain personal information about you such as pet's names, children's birth dates, or your anniversary
- B) You receive an invoice through email from what looks like a state employee's email address
- C) You receive a call from someone claiming to be an FBI agent asking for information on one of your inmates
- D) A stranger approaches you as you walk toward your building, starts a conversation, and follows you through the secure door

Question 9 of 25

Submit

True/False



Once CJIS has been extracted and entered into a CAD system, it no longer needs to be secure and it is okay to share this information with anyone that requests the information.

- A) True
- B) False

Question 10 of 25

Submit

Multiple Choice



Which of the following steps must be taken to ensure media protection?
(Select all that apply)

- A) CJI must be labeled and kept in a physically secure, locked area when not in use
- B) Mobile terminals should not be left unattended
- C) Computer monitors should be positioned facing toward windows or public access areas
- D) When transporting physical CJI, it must be hidden from view and only given to authorized personnel

Question 11 of 25

Submit

Multiple Choice



Select all of the information that is not allowed to be posted on social media.

- A) Criminal History records
- B) Names and social security numbers of people in your jail
- C) Employee personnel files
- D) All of the above

Question 12 of 25

Submit

Responsibilities in the CJIS system are set by the user's "need to know/need to share."

This means that your authorization to the systems that you access is based on your job assignment and the duties that you perform.

Users are not assigned access above their required level and are expected to access the system for work related purposes only. This means no "curiosity seeking" or surfing for information.



Click the forward button to continue.



A password is required to access the CJIS/CJIN system.

This means in addition to your domain password (i.e. windows) you'll also need a password to access CJIS systems. This includes interface devices like mobile terminals, CJIN computers, and federal CJI kiosks.

Your password must be kept secure, change frequently, and be unique to you.

NEVER share your password with anyone. No IT professional will ever ask for your password!

Click the forward button to continue.

Multiple Choice

Why is it considered bad practice to use the same password for all of the systems you access?

- A) Password requirements are different between systems
- B) Using the same password across systems is not a bad idea!
- C) Passwords must be changed every 60 days
- D) If your password is ever cracked, the hackers can access all of your accounts

Question 14 of 25

Multiple Choice

System access is given on a “need to know/need to share” basis meaning you are not given access to systems you don’t need to access for your job duties.

- A) True
- B) False

Question 13 of 25

Viruses, Trojan Horses, and other malicious codes affect us all.

These types of malicious code help hackers gain access to your systems.

Your agency must have malicious code protection that includes automatic updates for all systems with internet access. Software companies often include security updates when they push through their updates. By installing these updates, you ensure that your computer has the most recent patches and fixes to avoid malicious code.

If your IT Department has pushed through updates to your computer, please don't delay in installing them.



Click the forward button to continue.

Because law enforcement agencies in Montana are also connected to thousands of law enforcement agencies throughout the United States, system security is of the utmost importance.

DO NOT click on any links you are unfamiliar with or run any programs not authorized by your IT department. Viruses and Trojan Horses cannot work if you don't run their programs!

If you aren't sure about a program or link, call your supervisor or IT department before downloading or installing it.



If you ever suspect that your computer or the system has been compromised. Immediately contact your TAC and MT DOJ's Security Office by calling 406-444-3993.

Click the forward button to continue.

Multiple Choice



Why is it important to update your computer software whenever your IT department pushes through updates?

- A) It is not important to update your software
- B) The system will stop sending pop ups once you've updated
- C) Updates and patches frequently contain security updates
- D) Operating updated software always makes your computer run faster

Question 15 of 25

Multiple Choice



If you suspect a software install link you've been sent is untrustworthy and may be malicious in nature, what should you do?

- A) Click the link but run a virus scan once the software is installed
- B) Click the link and see where it goes
- C) Forward it to your friends to see if they will install the software
- D) Do not click on it, notify your supervisor or IT department

Question 16 of 25



Because email is the most common attack medium for social attacks, being able to spot fraudulent and malicious emails is a skill you need to possess.

Phishing emails will often contain grammatical mistakes, links embedded in the email that actually take you to a fake website, and generic greetings and signatures. You may notice an email from a supposed friend or colleague that doesn't have the personal tone that you're used to. These are definitely red flags.

According to Verizon's 2018 Data Breach Investigations Report (DBIR), 93% of all social breaches come from phishing and pretexting attacks. Email was the most common attack vector at 96%.



Click the forward button to continue.

Below are two email buttons. The email link to the left represents a .pdf of a fraudulent email from a scammer. The email link on the right represents a .pdf of a real email. Pay attention to the  logo on the pdf's for helpful hints in determining the validity of an email. Simply hover your cursor over the  to see the hints or right click the icon and select "open note."



Important!
If you ever have any question or doubt about the validity of an email you received, contact the sender by phone or another means other than email. They can confirm the accuracy of the email prior to you to taking any action!

Click the forward button to continue.

Multiple Choice

What are some of the areas to focus on in an email to determine whether or not the email is a possible phishing attack?

- A) Email length and sender
- B) Suspicious attachments, generic greeting, and embedded web links
- C) Email delivery time and lack of photos
- D) Topic, email length, and email delivery time

Question 17 of 25

Multiple Choice

Scenario 1 - Click the button to the right to view a sample email. Do you believe this email is legitimate or fraudulent?



- A) Definite scam
- B) I believe the email is legitimate

Question 18 of 25

Multiple Choice

Scenario 2 - Click the button to the right to view a sample email. Do you believe this email is legitimate or fraudulent?



- A) Definite scam
- B) I believe the email is legitimate

Question 19 of 25

Internet Use

Malicious websites are sites that attempt to install malware on your computer. This typically does require some action on your part. The web page could prompt you to download and install software that you aren't familiar with.

Malicious websites often mimic legitimate websites. Sometimes they'll ask you to install software that you appear to need to run a video or audio file. Never install something you aren't 100% certain on.

It is for this reason that internet use on computers interfaced with CJIS is strictly regulated to work-related purposes. This includes mobile terminals, interface devices, and Omnix machines. Since they all connect to CJIS, it is important to minimize risk whenever possible.

```

ws.on("message", m => {
  let a = m.split(" ");
  switch(a[0]){
    case "connect":
      if(a[1]){
        if(clients.has(a[1])){
          ws.send("connected");
          ws.id = a[1];
        }else{
          ws.id = a[1]
          clients.set(a[1], {client: {position: {x: 0, y: 0}, id: a[1]}});
          ws.send("connected")
        }
      }else{
        let id = Math.random().toString().slice(2, 8);
        ws.id = id;
        clients.set(id, {client: {position: {x: 0, y: 0}, id: id}});
      }
    }
  }
}

```

While CJIN requires internet use to be work-related purposes only, agencies can have policies that are more strict. Some agencies only allow their users to access approved websites or no web browsers at all. Be sure to know your agency's policy on internet use.

Click the forward button to continue.

According to Sitelock, there are more than 1.86 billion websites on the internet. Around 1% of these (approximately 18,500,000) are infected with malware at any given time.

By minimizing the websites you visit, you aid in keeping our network safe.



Click the forward button to continue.

Much like our desktop & laptop terminals, Mobile devices such as cell phones and tablets are also susceptible to attacks.

Some of the threats for mobile devices include:

- Loss, theft, or disposal
- Unauthorized access
- Malware
- Spam
- Electronic Eavesdropping
- Electronic tracking



Remember, hand-held devices often utilize bluetooth, infrared, cellular, and other wireless protocols that are capable of joining networks or creating their own networks. These networks can place your devices at risk. Never connect to a network you don't 100% trust!

Click the forward button to continue.

Multiple Choice

If a mobile terminal is interfaced with FBI CJIS, internet use on that computer is only permitted for work related purposes

- A) True
- B) False

Question 20 of 25

Submit

Spam

Spam messages are unsolicited messages, usually advertising, sent over several messaging systems. Spam can be found in emails, web search engines, online classified ads, text messages, and on social apps.

Agencies are required to install spam protection mechanisms to detect and take action on unsolicited messages but you won't be able to eliminate all Spam.

DO NOT click on any links or advertisements that you are not familiar with in your email. Many times clicking on links validates your email address to spammers thus making you a target for additional spam and phishing attacks.

- ▷ Inbox
- Drafts
- Sent Items
- Deleted Items
- Archive
- Conversation History
- Junk E-Mail**
- Outbox
- RSS Feeds
- ▷ Search Folders

Click the forward button to continue.

Physical Security of any device that handles CJJ is one of the most critical facets of system security.

All devices that contain CJJ must be stored in a physically secure location.

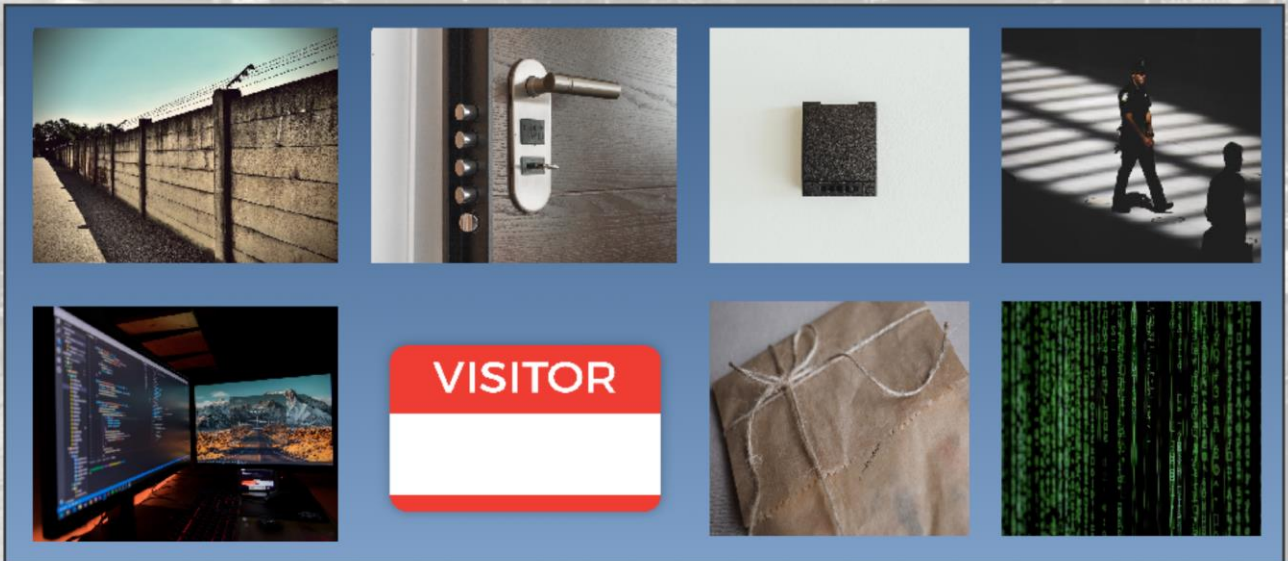
For a mobile terminal that means locked & docked inside a patrol car that is also secured and locked. For CJIN computers or servers, this means being in a locked area that the public or anyone not authorized to view CJJ, does not have access to.



A physically secure location is a facility, a criminal justice conveyance, or an area, a room, or a group of rooms within a facility with both the physical and personnel security controls sufficient to protect CJJ and associated information systems.

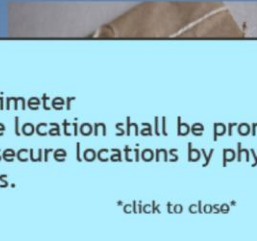
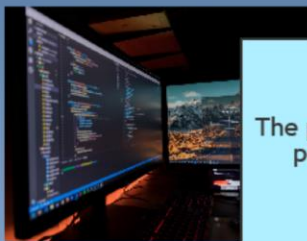
Click the forward button to continue.

The FBI has established eight criteria that define a physically secure area. Please click on the eight images below to view those criteria:



Click the forward button to continue.

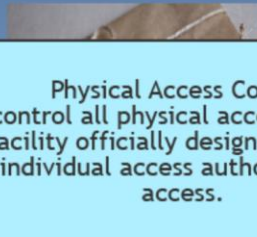
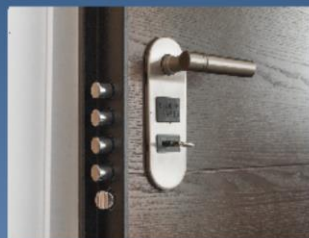
The FBI has established eight criteria that define a physically secure area.
Please click on the eight images below to view those criteria:



Security Perimeter
 The perimeter of a physically secure location shall be prominently posted and separated from non-secure locations by physical controls.
 click to close

Click the forward button to continue.

The FBI has established eight criteria that define a physically secure area.
Please click on the eight images below to view those criteria:



Physical Access Control
 The agency shall control all physical access points (except for those areas within the facility officially designated as publicly accessible) and shall verify individual access authorizations before granting access.
 click to close

Click the forward button to continue.

The FBI has established eight criteria that define a physically secure area. Please click on the eight images below to view those criteria:

Physical Access Authorization

The agency shall develop and keep current a list of personnel with authorized access to the physically secure location (except for those areas within the permanent facility officially designated as publicly accessible) or shall issue credentials to authorized personnel.

click to close

Click the forward button to continue.

The FBI has established eight criteria that define a physically secure area. Please click on the eight images below to view those criteria:

Monitoring Physical Access

The agency shall monitor physical access to the information system to detect and respond to physical security incidents.

click to close

Click the forward button to continue.

The FBI has established eight criteria that define a physically secure area.
Please click on the eight images below to view those criteria:



Access Control for Display
 The agency shall control physical access to information system devices that display CJI and shall position information system devices in such a way as to prevent unauthorized individuals from accessing and viewing CJI.
 click to close

Click the forward button to continue.

The FBI has established eight criteria that define a physically secure area.
Please click on the eight images below to view those criteria:



Visitor Control
 The agency shall control physical access by authenticating visitors before authorizing escorted access to the physically secure location (except for those areas designated as publicly accessible). The agency shall escort visitors at all times and monitor visitor activity.
 click to close

Click the forward button to continue.

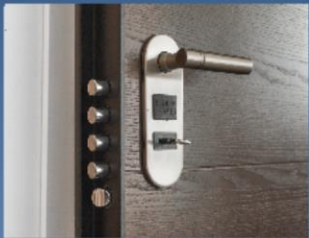
The FBI has established eight criteria that define a physically secure area. Please click on the eight images below to view those criteria:

Delivery and Removal
The agency shall authorize and control information system-related items entering and exiting the physically secure location.
click to close



Click the forward button to continue.

The FBI has established eight criteria that define a physically secure area. Please click on the eight images below to view those criteria:



Access Control for Transmission
The agency shall control physical access to information system distribution and transmission lines within the physically secure location.
click to close

Click the forward button to continue.

Personally Owned Equipment



Any personally owned information system shall not be authorized to access, process, store, or transmit CJ unless the agency has established specific terms, conditions, and policy for their usage.

This also applies for personally owned equipment like flash drives, hard drives, or CD's/DVD's. If you are going to use these forms of equipment, make sure you have prior approval.

Click the forward button to continue.

Individual Accountability

Individual Accountability means that you are accountable for all of your actions. You are expected to perform queries and use the system in accordance with FBI CJIS, CJIN, and your own agency's policies. Every query you make in the system is recorded and can be audited at any time.



**I WILL FIND
YOU....**

**AND I WILL
AUDIT YOU**



Click the forward button to continue.

Acknowledgment Statements

Acknowledgment statements are used to document and acknowledge the receipt and understanding of information. We see these statements with HR forms, privacy notices, and even computer programs.

These are the statements that explain the rules of the system you are accessing. Many of these statements will include why you have access to the systems and data that you do, what the purpose of the data is, and the consequences of misusing the privileges given.

They will also mention not using the system for any kind of personal use or gain and keeping your password to yourself.

Every time you click “Ok” or “Acknowledge”, you are agreeing to the conditions set forth by the statement.



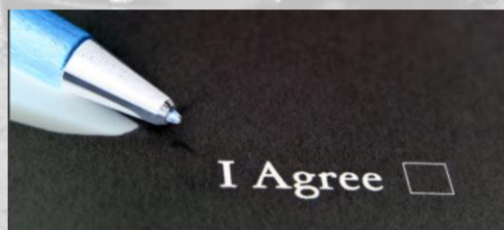
Click the forward button to continue.

Acknowledgment Statements

Think back on the systems you access, how many of them have acknowledgment statements? What do these statements entail?

For example, any system that connects to CJIN must have users acknowledge:

- ❖ The user is accessing a restricted information system
- ❖ System usage may be monitored, recorded, and subject to audit
- ❖ Unauthorized use of the system is prohibited and may be subject to criminal and/or civil penalties
- ❖ Use of the system indicates consent to monitoring and recording



Click the forward button to continue.



Our computers enable us to receive protected criminal justice information in a matter of seconds. It is important to keep that information secure, even in an office environment.

FBI CJIS policy states that computers on the system must have a 30 minute session lock. This means the computer locks after 30 minutes of inactivity. System locks need to be in place to prevent inadvertent viewing when your device is unattended. One of the most basic types of screen lock is the screensaver.

Screensavers used to serve the purpose of preventing burn-in images on computer monitors. With the advent of new monitor technology, screensavers now help prevent any unauthorized viewing of your desktop.

Click the forward button to continue.

In addition to a screen saver, it's a good practice to use a privacy screen. Privacy screens are polarized sheets of plastic that prevent visibility from angles that are not straight on. By utilizing a privacy screen, you can help avoid "shoulder surfing" and wandering eyes. Be sure that people that are viewing your screen are authorized access to the systems and the information contained in those systems. If you are issued a battery backup device, be sure to use it to prevent the loss of data in the event of an emergency.



Click the forward button to continue.

Matching



Match the following terms and their definitions:

Terms

- Physically Secure Location
- Individual Accountability
- Spam
- Acknowledgment Statement

Definitions

- A) Document and acknowledge the receipt of information
- B) Unsolicited messages, usually advertisements
- C) A place with controls sufficient to protect CJJ
- D) You are accountable for all of your actions
- E) Biometric data

Question 21 of 25

Submit

Multiple Choice



Select all possible ways to protect the data on your computer.

- A) Privacy screens
- B) Monitor dimness setting at 15%
- C) Physical security (stored in a secure location)
- D) Screen lock (Screen saver)

Question 22 of 25

Submit

It is your responsibility to protect sensitive information. Remember this information can be stored in your CAD/RMS system, on archive/backup software, and portable media.

Any devices or systems that store sensitive information must be kept in a physically secure location. This can include portable hard drives, flash drives, CD's, DVD's, or memory cards.

Your responsibility does not end until the sensitive information is disposed of properly. For physical media, this means data destruction. For digital media, this will be sanitation.



Click the forward button to continue.



Sanitization is either overwriting at least three times or degaussing digital media prior to disposal or reuse.

Any inoperable digital media, such as a broken hard drive, needs to be destroyed (cut up, shredded, etc.)

Your agency is responsible for maintaining written documentation of the steps taken to sanitize or destroy electronic media. This process needs to be witnessed or carried out by authorized personnel.

Click the forward button to continue.

Physical media needs to be securely disposed of when it is no longer required.

Formal procedures are necessary to minimize the risk of sensitive information getting into the wrong hands.

Physical media needs to be either shredded or incinerated. It is the agency's responsibility to ensure that the destruction is witnessed or carried out by authorized personnel.



Click the forward button to continue.



Due to the nature of your job and the sensitive material you have access to, you can be a target for criminals hoping to gain access to that material.

There are two main approaches criminals will use to try to gain access to the system through you - Social Engineering and through your computer programs or hardware.

As discussed before, Social engineering is when a group or an individual attempts to trick you into providing them information.

The second attack vector would be from your computer. Installing unfamiliar or dangerous desktop programs or applications, using unauthorized flash drives or hard drives, and downloading dangerous add ons can all leave you and the system exposed.

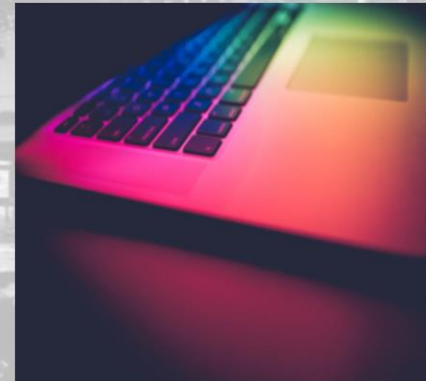
Click the forward button to continue.

Effective patch management and anti-virus software are required for CJIS computers.

For patch management, local policies must include:

- Testing of appropriate patches before installation
- Rollback capabilities when installing patches, updates, etc
- Automatic updates without individual user intervention
- Centralized patch management

Any patch requirements discovered during security assessments, continuous monitoring, or incident response activities need to be addressed expeditiously.



Click the forward button to continue.



System patches must be installed in a timely manner because patches are critical in fixing security vulnerabilities or other bugs.

This means going through the steps of installing them on a test system, confirming they work, troubleshooting any potential issues, and installing them on the production systems.

The testing component is important because poorly designed or rushed patches can sometimes introduce new problems.

Click the forward button to continue.

Multiple Choice

Your responsibility in handling sensitive Criminal Justice Information does not end until:

- A) You turn the data over to someone else
- B) Your responsibility doesn't end, it's a lifelong commitment
- C) You are finished accessing the data
- D) The sensitive information is disposed of properly

Question 23 of 25

Multiple Choice

Which are the two main approaches criminals use to gain access to the system through you (select all that apply):

- A) Through your computer programs or hardware
- B) Through federal mail scams
- C) Through social engineering
- D) Through phone conferencing

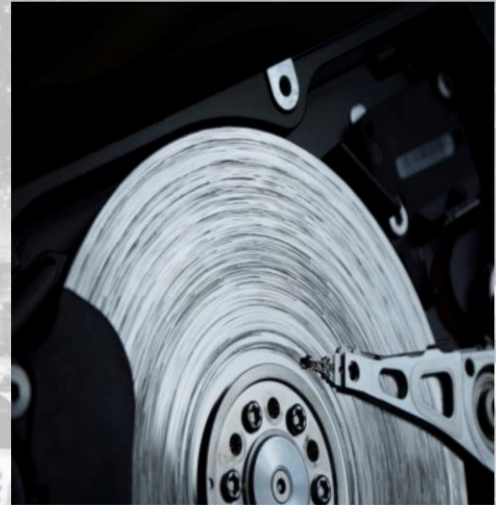
Question 24 of 25

Data Backup

There are two approaches to data backup and storage. Centralized or decentralized.

A centralized approach replicates data from remote sites and sends it over a network to a main (centralized) location for storage. This type of backup can be used to automate backups at remote sites.

A decentralized approach involves data being stored on multiple computers hosted by participants cooperating on a network. One example of this is Cloud storage.



Regardless of which approach your agency takes, Data Storage must comply with FBI CJIS policy.

Click the forward button to continue.

Network Infrastructure Protection

Network Infrastructure is one of the key areas where the system needs to remain secure. This not only means physical and virtual security, but also who is accessing the system and from where.

Some of the requirements include:

- Controlling log-in information
- Enforcing regular password changes
- Two-Factor Authentication when necessary
- Regular virus and malware scanning
- Patches and updates when available
- Robust firewall system



Click the forward button to continue.

Multiple Choice

What is NOT one of the requirements for a secure network infrastructure?

- A) Two-Factor authentication when necessary
- B) Robust firewall system
- C) A notebook containing written IP addresses for your network
- D) Regular virus and malware scanning

Question 25 of 25

Quiz Results



Sorry, you failed

You Scored:
Maximum Score:
Correct Questions:
Total Questions:
Accuracy:
Attempts:

-
-
-