

# Cjis Security Awareness Test Answers

---

## Level 2 CJIS Security Test questions with correct answers

The CJIS Security Policy outlines the minimum requirements. Each criminal justice agency is encouraged to develop internal security training that defines local and agency specific policies and procedures. - correct answer True

What agencies should have written policy describing the actions to be taken in the event of a security incident? - correct answer Every agency accessing CJI

Criminal History Record Information (CHRI) is arrest-based data and any derivative information from that record. - correct answer True

During social engineering, someone pretends to be \_\_\_\_\_ in an attempt to gain illicit access to protected data systems. - correct answer an authorized user or other trusted source

Who should report any suspected security incident? - correct answer All personnel

Hard copies of CJI data should be \_\_\_\_\_ when no longer required. - correct answer physically destroyed

Users do not need to log off of the software/system at the end of the shift or when another operator wants to use the software/system. - correct answer False

Agencies are not required to develop and publish internal information security policies, including penalties for misuse. - correct answer False

Custodial workers that access the terminal area must have a fingerprint background check done and training unless they are escorted in these areas. - correct answer True

Training for appropriate personnel would include people who read criminal histories but do not have a NCIC workstation of their own. - correct answer True

CJIS security awareness test answers are crucial for individuals working with law enforcement agencies and those handling criminal justice information. The Criminal Justice Information Services (CJIS) Division of the FBI has established security requirements to protect sensitive data. Understanding these requirements and the correct responses to security awareness tests is essential for ensuring compliance and maintaining the integrity of the information.

# Introduction to CJIS Security Requirements

The CJIS Security Policy outlines a framework to ensure the confidentiality, integrity, and availability of criminal justice information. This policy is applicable to all agencies that access or store such information. Security awareness training is a key component of this framework, as it educates personnel on best practices and potential threats.

## Importance of CJIS Security Awareness Training

- **Protection of Sensitive Information:** The primary goal of CJIS security training is to safeguard sensitive data from unauthorized access and breaches.
- **Legal Compliance:** Agencies must comply with federal and state laws regarding the handling of criminal justice information. Regular training ensures adherence to these regulations.
- **Risk Mitigation:** By educating employees about potential security threats, agencies can reduce the risk of data breaches and cyberattacks.
- **Incident Response Preparedness:** Training prepares staff to respond effectively to security incidents, minimizing damage and facilitating quicker recovery.

## Common Topics Covered in CJIS Security Awareness Tests

CJIS security awareness tests often cover a variety of topics that are vital for maintaining security within law enforcement agencies. Here are some key areas typically included:

### 1. Data Security Principles

Understanding the fundamental principles of data security is essential. Key concepts include:

- **Confidentiality:** Ensuring that sensitive information is only accessible to authorized individuals.
- **Integrity:** Protecting data from unauthorized alterations or deletions.
- **Availability:** Ensuring that data is accessible when needed by authorized users.

## **2. Password Management**

Effective password management is critical for protecting information systems. Training usually emphasizes the following practices:

- Creating Strong Passwords: Use a mix of letters, numbers, and special characters.
- Changing Passwords Regularly: Regular updates help mitigate the risk of unauthorized access.
- Avoiding Password Sharing: Passwords should never be shared, even among colleagues.
- Using Multi-Factor Authentication (MFA): Enhances security by requiring additional verification methods.

## **3. Recognizing Phishing Attempts**

Phishing is a prevalent threat that targets individuals to gain unauthorized access to systems. Training covers:

- Identifying Suspicious Emails: Look for unusual sender addresses and poor grammar.
- Avoiding Clicking on Links: Always verify the legitimacy of links before clicking.
- Reporting Phishing Attempts: Employees should know how to report suspicious emails to their IT departments.

## **4. Physical Security Measures**

Physical security is just as important as cyber security. Key measures include:

- Securing Workstations: Locking computers when not in use to prevent unauthorized access.
- Controlling Access to Sensitive Areas: Ensuring only authorized personnel can enter secure locations.
- Monitoring Visitors: Keeping track of who enters and exits secure facilities.

## **5. Secure Use of Mobile Devices**

With the increasing use of mobile devices, understanding their security is critical:

- Encrypting Sensitive Data: Ensures data is protected if a device is lost or stolen.

- Using Secure Connections: Always use a Virtual Private Network (VPN) when accessing sensitive information remotely.
- Regularly Updating Software: Keeping devices updated helps protect against vulnerabilities.

## **Best Practices for CJIS Compliance**

To maintain compliance with CJIS security policies, agencies should implement best practices, which include:

### **1. Regular Training and Testing**

- Frequent Updates: Security training should be updated regularly to reflect new threats and technologies.
- Mandatory Participation: All personnel should be required to complete security awareness training.
- Testing Understanding: Regular assessments and quizzes can help gauge the effectiveness of training.

### **2. Incident Reporting Protocols**

- Establish Clear Procedures: Employees should know how to report security incidents promptly.
- Encourage Transparency: Foster a culture where employees feel comfortable reporting potential security threats without fear of repercussions.

### **3. Develop a Security Policy Manual**

- Comprehensive Documentation: A manual detailing security policies and procedures should be readily available to all employees.
- Regular Reviews: Policies should be reviewed and updated periodically to reflect current best practices and regulations.

### **4. Conduct Security Audits**

- Regular Assessments: Agencies should conduct audits to evaluate the effectiveness of their security measures.

- **Identify Vulnerabilities:** Audits help uncover potential weaknesses that need to be addressed.

## **Conclusion**

CJIS security awareness test answers provide a vital resource for individuals working within the criminal justice system. By understanding the key principles of data security, password management, phishing recognition, physical security, and mobile device usage, employees can contribute to the protection of sensitive information.

Moreover, adhering to best practices for CJIS compliance, such as regular training, incident reporting, maintaining a security policy manual, and conducting audits, helps create a robust security culture within agencies. Ultimately, the goal is to ensure that criminal justice information remains secure and that personnel are equipped to handle potential threats effectively. As technology evolves, ongoing education and adherence to security protocols will be paramount in safeguarding sensitive data in the criminal justice field.

## **Frequently Asked Questions**

**What does CJIS stand for?**

CJIS stands for Criminal Justice Information Services.

**Why is security awareness training important for CJIS?**

**Security awareness training is crucial for CJIS to protect sensitive criminal justice information from unauthorized access and breaches.**

**What is the primary focus of the CJIS Security Awareness Test?**

**The primary focus of the CJIS Security Awareness Test is to ensure that personnel understand the policies and procedures for safeguarding criminal justice information.**

**What are some common topics covered in the CJIS Security Awareness Test?**

**Common topics include data protection, password management, social engineering, and incident reporting.**

**What should you do if you encounter a phishing attempt while working with CJIS data?**

**You should report the phishing attempt to your IT department or designated security officer immediately.**

**How often should CJIS security awareness training be conducted?**

**CJIS security awareness training should be conducted at least annually, or more frequently if significant changes occur in policies or technology.**

**What is the consequence of failing the CJIS Security Awareness Test?**

**Failing the CJIS Security Awareness Test may require individuals to retake the training until they**

demonstrate an understanding of security protocols.

Find other PDF article:

<https://soc.up.edu.ph/05-pen/files?trackid=dKL10-1562&title=amazing-animal-facts-for-kids.pdf>

## Cjis Security Awareness Test Answers

### State Identification Bureau Listing – FBI

Illinois State Police 260 North Chicago Street  
Joliet, IL 60432-4075 (815) 740-5160 Indiana Records  
Division Indiana State Police Indiana ...

### Criminal Justice Information Services (CJIS) Security Policy

Dec 20, 2023 · EXECUTIVE SUMMARY Law enforcement  
needs timely and secure access to services that  
provide data wherever and ...

Criminal Justice Information Services (CJIS) – FBI  
The FBI's Criminal Justice Information Services  
Division, or CJIS, is a high-tech hub in the hills  
of West Virginia that provides a range of state of ...

### FBI Releases 2023 Crime in the Nation Statistics – FBI

Sep 23, 2024 · The FBI released detailed data on  
over 14 million criminal offenses for 2023 reported  
to the Uniform Crime Reporting (UCR) ...

## ***NIBRS User Manual 2025.0 – LE***

**NIBRS User Manual 2025-0Download nibrs-user-manual-2025-0-062625.pdf – 3147 KB Informational Tools Uniform Crime Reports ...**

## ***State Identification Bureau Listing – FBI***

**Illinois State Police 260 North Chicago Street  
Joliet, IL 60432-4075 (815) 740-5160 Indiana Records  
Division Indiana State Police Indiana Government  
Center, North 100 North Senate ...**

## **Criminal Justice Information Services (CJIS)**

### **Security Policy**

**Dec 20, 2023 · EXECUTIVE SUMMARY Law enforcement needs timely and secure access to services that provide data wherever and whenever for stopping and reducing crime. In ...**

## **Criminal Justice Information Services (CJIS) – FBI**

**The FBI's Criminal Justice Information Services Division, or CJIS, is a high-tech hub in the hills of West Virginia that provides a range of state of-the-art tools and services to law ...**

## **FBI Releases 2023 Crime in the Nation Statistics – FBI**

**Sep 23, 2024 · The FBI released detailed data on over 14 million criminal offenses for 2023 reported to the Uniform Crime Reporting (UCR) Program by participating law enforcement ...**

## **NIBRS User Manual 2025.0 – LE**

**NIBRS User Manual 2025-0Download nibrs-user-manual-2025-0-062625.pdf – 3147 KB Informational**



**Tools Uniform Crime Reports National Crime  
Information Center (NCIC) Law ...**

**FBI – Table 8 - Illinois**

**Home • Crime in the U.S. • 2012 • Crime in the U.S.  
2012 • Tables • 8TableDataDecPDF • Table 8 State  
cuts • Table 8 - Illinois Criminal Justice  
Information Services Division**

**Contact Us – FBI**

**Please contact your local FBI office to submit a tip  
or report a crime. Use our online form to file  
electronically or call the appropriate toll-free  
number.**

**List of Approved Channelers – FBI**

**Dec 13, 2024 · A listing of approved companies  
providing Channeler services for agencies.**

***FBI – Federal Bureau of Investigation***

**We protect the American people and uphold the US  
Constitution. You can report suspicious activities  
and crime by contacting us 24/7 at [tips.fbi.gov](https://tips.fbi.gov).**

**FBI – Illinois**

**Home • Crime in the U.S. • 2019 • Crime in the U.S.  
2019 • Tables • Table 8 • Table 8 state cuts •  
Illinois Criminal Justice Information Services  
Division**

**Unlock essential insights with our comprehensive  
guide on CJIS security awareness test answers. Boost**

**your knowledge and compliance today! Learn more.**

**[Back to Home](#)**