NMDPS NATIONAL CRIME INFORMATION CENTER (NCIC) PRACTICE EXAM (SAMPLE)

STUDY GUIDE

SAMPLE STUDY GUIDE WITH LIMITED QUESTIONS

VISIT US ONLINE FOR THE FULL VERSION STUDY GUIDE

https://nmpdsncic.examzify.com

Table of Contents

Introduction

Preparing for a certification exam can feel overwhelming, but with the right tools, it becomes an opportunity to build confidence, sharpen your skills, and move one step closer to your goals. At Examzify, we believe that effective exam preparation isn't just about memorization, it's about understanding the material, identifying knowledge gaps, and building the test-taking strategies that lead to success.

This guide was designed to help you do exactly that.

Whether you're preparing for a licensing exam, professional certification, or entry-level qualification, this book offers structured practice to reinforce key concepts. You'll find a wide range of multiple-choice questions, each followed by clear explanations to help you understand not just the right answer, but why it's correct.

The content in this guide is based on real-world exam objectives and aligned with the types of questions and topics commonly found on official tests. It's ideal for learners who want to:

- Practice answering questions under realistic conditions,
- Improve accuracy and speed,
- Review explanations to strengthen weak areas, and
- Approach the exam with greater confidence.

We recommend using this book not as a stand-alone study tool, but alongside other resources like flashcards, textbooks, or hands-on training. For best results, we recommend working through each question, reflecting on the explanation provided, and revisiting the topics that challenge you most.

Remember: successful test preparation isn't about getting every question right the first time, it's about learning from your mistakes and improving over time. Stay focused, trust the process, and know that every page you turn brings you closer to success.

Let's begin.

How to Use This Guide

This guide is designed to help you study more effectively and approach your exam with confidence. Whether you're reviewing for the first time or doing a final refresh, here's how to get the most out of your Examzify study guide:

1. Start with a Diagnostic Review

Skim through the questions to get a sense of what you know and what you need to focus on. Your goal is to identify knowledge gaps early.

2. Study in Short, Focused Sessions

Break your study time into manageable blocks (e.g. 30 – 45 minutes). Review a handful of questions, reflect on the explanations.

3. Learn from the Explanations

After answering a question, always read the explanation, even if you got it right. It reinforces key points, corrects misunderstandings, and teaches subtle distinctions between similar answers.

4. Track Your Progress

Use bookmarks or notes (if reading digitally) to mark difficult questions. Revisit these regularly and track improvements over time.

5. Simulate the Real Exam

Once you're comfortable, try taking a full set of questions without pausing. Set a timer and simulate test-day conditions to build confidence and time management skills.

6. Repeat and Review

Don't just study once, repetition builds retention. Re-attempt questions after a few days and revisit explanations to reinforce learning. Pair this guide with other Examzify tools like flashcards, and digital practice tests to strengthen your preparation across formats.

There's no single right way to study, but consistent, thoughtful effort always wins. Use this guide flexibly, adapt the tips above to fit your pace and learning style. You've got this!

Questions

1. Which of the following is NOT included in electronic media?

A. USBs

B. Fax machines

C. Hard drives

D. Tape

2. Which of the following is not an acceptable entry for the REASON field when running a III?

A. An agency case number

B. A random identifier

C. A criminal warrant

D. A pending investigation

3. What specific information is typically included in a wanted person's NCIC entry?

A. Name, photograph, last known address, and warrant details

B. Criminal history and fingerprints

C. Earnings history and bank account information

D. All known aliases and driver's license numbers

4. What is the NCIC's role in gang-related investigations?

A. To provide data on known gang members and their activities

B. To compile crime statistics

C. To train law enforcement officers

D. To conduct undercover operations

5. False statement regarding FBI CJIS data/CHRI is:

A. It includes only personal identifiable information.

B. It is subject to confidentiality regulations.

C. It must not be publicly accessible.

D. All users can access it without training.

6. Are records in the NCIC accessible to the general public?

A. Yes, it's open to all

B. No, access is restricted to authorized personnel only

C. Only under specific conditions

D. Yes, but only for a fee

7. What is a primary limitation of the data shared through NCIC?

A. It's available for all public use

B. It is only for criminal justice purposes

C. It's only for administrative use

D. It cannot be shared between local agencies

8. True or False: All electronic media are considered secure without additional protection.

A. True

B. False

C. Sometimes True

D. None of the above

9. Which of the following hot files contains CHRI?

A. Convicted Felon List

B. Known or appropriately suspected terrorist (KST) file

C. Missing Person File

D. Unregistered Vehicle File

10. Is it necessary for users to log off software/systems at the end of their shift?

A. Yes, always

B. No, it's optional

C. Only if instructed

D. Only for critical systems

Answers

1. B
2. B
3. A
4. A
5. D
6. B
7. B
8. B
9. B
10. B

Explanations

1. Which of the following is NOT included in electronic media?

A. USBs

B. Fax machines

C. Hard drives

D. Tape

Fax machines are not considered electronic media in the same sense as the other options. Electronic media typically refers to devices that store, process, and transmit digital information. USBs, hard drives, and tapes all function as storage mediums for digital data, allowing for the retrieval and manipulation of that data within electronic devices. USBs are portable storage devices that connect to computers, hard drives serve as major data storage components for computers and other devices, and tapes (such as magnetic tapes) are used for storing large amounts of data, often for backup purposes. Fax machines, on the other hand, are primarily telecommunications devices that transmit printed material over phone lines, functioning more as a means of communication rather than as a medium for electronic data storage and processing. This distinction helps clarify why fax machines do not fit the category of electronic media as defined in this context.

2. Which of the following is not an acceptable entry for the REASON field when running a III?

A. An agency case number

B. A random identifier

C. A criminal warrant

D. A pending investigation

The correct choice is a random identifier, as it does not provide meaningful context or linkage to a legitimate law enforcement reason for accessing the criminal history information. The REASON field is designed to capture specific information that justifies the request for accessing a person's criminal history. Acceptable entries should be relevant and pertinent to the law enforcement purpose. In contrast, an agency case number, a criminal warrant, and a pending investigation all serve as appropriate entries. They indicate a clear and traceable law enforcement purpose, which is essential in maintaining the integrity and accountability of law enforcement operations when accessing sensitive information in the Interstate Identification Index (III). These entries support the necessity of obtaining criminal history records and ensure that requests are filed under legitimate circumstances as outlined by legal requirements and agency protocols.

3. What specific information is typically included in a wanted person's NCIC entry?

A. Name, photograph, last known address, and warrant details

B. Criminal history and fingerprints

C. Earnings history and bank account information

D. All known aliases and driver's license numbers

The inclusion of a person's name, photograph, last known address, and warrant details in an NCIC entry is essential for the identification and apprehension of wanted individuals. The name ensures that law enforcement personnel can readily identify the individual. The photograph provides a visual aid to support recognition, which is especially important in cases where the person may not be easily identifiable by name alone. The last known address allows officers to trace the individual's whereabouts or establish a connection to a specific area, while warrant details inform law enforcement about the nature of the offenses for which the individual is wanted, including the type of warrant, the issuing agency, and the charges involved. In contrast, while criminal history and fingerprints are crucial for thorough background checks, they are not typically part of the basic NCIC entry for a wanted person. The profiling of earnings and bank account information does not contribute to the identification or apprehension process and is not included either. Lastly, while knowing aliases and driver's license numbers can be useful, the more critical and immediate information for law enforcement is the basic identifying details and warrant specifics that are included in option A.

4. What is the NCIC's role in gang-related investigations?

A. To provide data on known gang members and their activities

B. To compile crime statistics

C. To train law enforcement officers

D. To conduct undercover operations

The National Crime Information Center (NCIC) plays a crucial role in gang-related investigations primarily by providing data on known gang members and their activities. This data is essential for law enforcement agencies as it enables them to identify affiliations, track movements, and monitor the activities of individuals involved in gang-related activities. The information gathered by the NCIC includes details about gang membership and associations, which can lead to more effective policing strategies and coordinated responses to gang violence. In essence, this function directly supports investigations and helps in formulating a comprehensive approach to combat gang-related crime. The other options, while relevant to law enforcement and crime prevention, do not reflect the specific function of NCIC in the context of gang-related investigations. Compiling crime statistics is a broader function that may not focus exclusively on gangs, training law enforcement officers falls outside the database function of NCIC, and conducting undercover operations is typically the responsibility of individual law enforcement agencies rather than a function of NCIC.

5. False statement regarding FBI CJIS data/CHRI is:

A. It includes only personal identifiable information.

B. It is subject to confidentiality regulations.

C. It must not be publicly accessible.

D. All users can access it without training.

The assertion that all users can access FBI CJIS data or Criminal History Record Information (CHRI) without training is false. Accessing this sensitive information requires specialized training, as the data includes personal identifiable information that is highly confidential. Proper handling of such data is critical to protect individuals' privacy rights and to comply with federal regulations regarding the dissemination and use of criminal justice information. Training ensures that users understand the protocols for accessing, sharing, and maintaining the security of this information. It equips them to recognize the legal and ethical responsibilities involved, as well as the potential consequences of misuse. This required training reflects the importance of safeguarding sensitive data in law enforcement and criminal justice contexts.

6. Are records in the NCIC accessible to the general public?

A. Yes, it's open to all

B. No, access is restricted to authorized personnel only

C. Only under specific conditions

D. Yes, but only for a fee

The correct answer highlights that records in the NCIC are restricted to authorized personnel only. This restriction is crucial for maintaining the integrity and confidentiality of sensitive criminal justice information. The NCIC (National Crime Information Center) serves law enforcement agencies and provides vital data related to wanted persons, stolen property, and other criminal justice information which must be protected to prevent misuse and ensure privacy. Access limitations are in place to ensure that only those with legitimate law enforcement purposes have the ability to retrieve information. This protection helps maintain public trust in the criminal justice system and ensures that information is not misused by individuals who may have ulterior motives. In contrast, the other options suggest different levels of accessibility that do not align with the operational principles of the NCIC. The notion of public access, whether completely open, under specific conditions, or for a fee, overlooks the critical need for controlled access to sensitive data. This helps safeguard individuals' rights and protects the integrity of investigations and law enforcement processes.

7. What is a primary limitation of the data shared through NCIC?

A. It's available for all public use

B. It is only for criminal justice purposes

C. It's only for administrative use

D. It cannot be shared between local agencies

The primary limitation of the data shared through NCIC being restricted to criminal justice purposes is crucial to understanding the framework and integrity of the system. NCIC, which stands for the National Crime Information Center, is designed to assist law enforcement and criminal justice agencies in the processing and analysis of criminal information. This limitation ensures that the data is used solely for legitimate law enforcement activities, enhancing the protection of sensitive information and maintaining the privacy rights of individuals. By limiting access to authorized entities engaged in criminal justice, NCIC helps prevent misuse of the data, ensuring it supports public safety efforts effectively. The other options do not accurately describe the restrictions in the context of NCIC's operation. The fact that data is not available for all public use highlights the importance placed on accountability and controlled access, while the distinction that it is not purely for administrative use emphasizes its dedicated focus on law enforcement functions. Additionally, while local agencies may share information, the emphasis is more on the purpose of the access rather than outright prohibition, which is why the focus on criminal justice use is a critical element of NCIC's limitations.

8. True or False: All electronic media are considered secure without additional protection.

A. True

B. False

C. Sometimes True

D. None of the above

The statement that all electronic media are considered secure without additional protection is false. This highlights the understanding that inherent security is not guaranteed simply by the nature of the medium itself. Electronic media, including computers, servers, and various storage devices, may contain vulnerabilities that can be exploited by malicious actors. Security measures such as encryption, firewalls, and access controls are essential to protect the integrity and confidentiality of data stored on electronic media. Without these additional layers of protection, data can be susceptible to risks such as unauthorized access, data breaches, and cyberattacks. Recognizing that not all electronic media are inherently secure emphasizes the importance of proactive security practices in safeguarding sensitive information and maintaining data security standards.

9. Which of the following hot files contains CHRI?

A. Convicted Felon List

B. Known or appropriately suspected terrorist (KST) file

C. Missing Person File

D. Unregistered Vehicle File

The correct response to the question is the Known or Appropriately Suspected Terrorist (KST) file. This file contains Criminal History Record Information (CHRI) pertinent to individuals who are known to or appropriately suspected of engaging in activities aligned with terrorism. The importance of this classification lies in its role in national security and law enforcement strategies, allowing agencies to identify potential threats and individuals who may pose a risk. The other files mentioned do not specifically pertain to CHRI. For example, while the Convicted Felon List provides a record of individuals who have been convicted of felonies, it does not necessarily encompass the broader category of CHRI as linked to terrorism activity, which is what the KST file addresses. Similarly, the Missing Person File contains information related to individuals who are missing and their associated cases but does not include specific criminal histories. Lastly, the Unregistered Vehicle File focuses on vehicles rather than individuals and their criminal records, making it irrelevant in the context of CHRI. Thus, the KST file stands out as the one explicitly associated with CHRI.

10. Is it necessary for users to log off software/systems at the end of their shift?

A. Yes, always

B. No, it's optional

C. Only if instructed

D. Only for critical systems

The importance of logging off software or systems at the end of a shift primarily revolves around security and data integrity. Logging off ensures that unauthorized individuals cannot access sensitive information or perform actions within the system using someone else's credentials. This practice helps protect against potential security breaches and maintains the confidentiality of the data handled during the shift. While it may seem that it could be optional to log off, in practice, it is a best practice often mandated for various systems, especially those handling sensitive or personal data. Leaving a session open may expose critical information to unintended users, posing a risk to the organization. In contrast to the selected answer that suggests it is optional, the most appropriate response would emphasize that logging off is a necessary practice to uphold security protocols. Ensuring that every user logs off after their shift contributes significantly to overall system safety and integrity and aligns with many organizations' IT security policies.

Next Steps

Congratulations on reaching the final section of this guide. You've taken a meaningful step toward passing your certification exam and advancing your career.

As you continue preparing, remember that consistent practice, review, and self-reflection are key to success. Make time to revisit difficult topics, simulate exam conditions, and track your progress along the way.

If you need help, have suggestions, or want to share feedback, we'd love to hear from you. Reach out to our team at hello@examzify.com.

Or visit your dedicated course page for more study tools and resources:

https://nmpdsncic.examzify.com

We wish you the very best on your exam journey. You've got this!