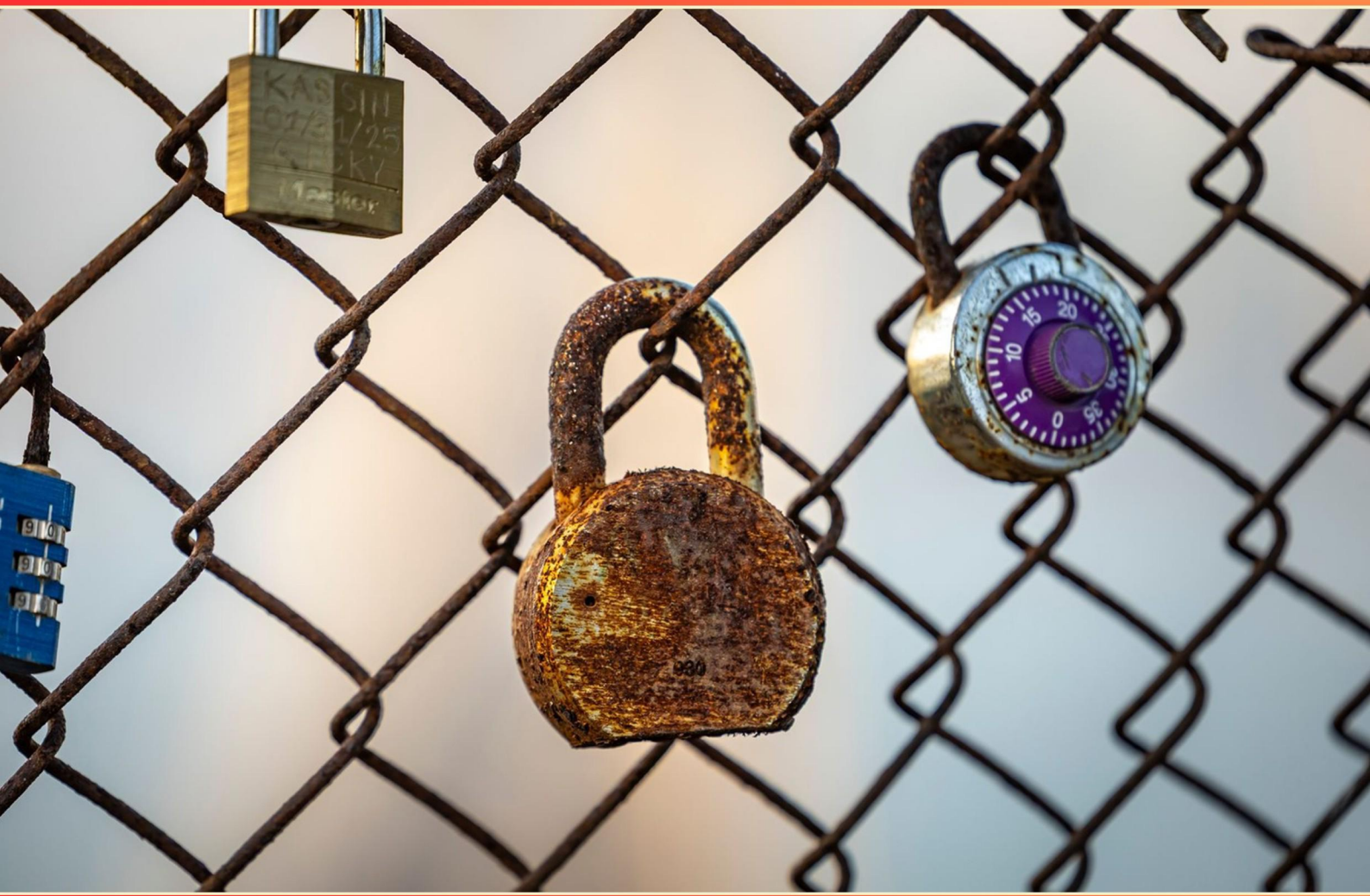
DOD INSTRUCTION 5200.48 CONTROLLED UNCLASSIFIED INFORMATION (CUI) PRACTICE EXAM (SAMPLE)

STUDY GUIDE



SAMPLE STUDY GUIDE WITH LIMITED QUESTIONS

VISIT US ONLINE FOR THE FULL VERSION STUDY GUIDE

https://dodinstruction520048cui.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. **What is the high-level message about information sharing versus controls in the CUI program?**

   A. The program aims to promote sharing as much as possible while maintaining required safeguarding/handling measures.

   B. The program prioritizes safeguarding over sharing.

   C. The program aims to completely prohibit sharing.

   D. The program aims to promote sharing as much as possible while maintaining required safeguarding/handling measures.

2. **How is CUI incident response integrated with the broader incident handling process?**

   A. CUI incidents are managed separately from general incident handling.

   B. There is no requirement for reporting CUI incidents.

   C. The CUI incident response is integrated into the broader incident handling process to ensure prompt reporting and mitigation.

   D. CUI incident response is handled exclusively by the IT department.

3. **Under DoD public release processes, when is DoD CUI considered controlled?**

   A. Until authorized for public release under DoD public release processes.

   B. Indefinitely.

   C. Only during maintenance.

   D. Only when stored in approved devices.

4. **What does 'dissemination controls' mean in CUI handling?**

   A. Destruction timing.

   B. Limits on how, where, and to whom CUI can be disclosed or shared.

   C. Encryption standards only.

   D. Only for printing and distribution.

5. **What is the primary purpose of DoD Instruction 5200.48 regarding CUI within the DoD?**

   A. To classify all information as top secret

   B. To define encryption standards for all DoD systems

   C. To establish policy and responsibilities for designation, safeguarding, marking, dissemination, decontrol, and destruction of CUI within DoD.

   D. To regulate personnel security clearances across DoD

6. What is the purpose of the DoD CUI Registry?

A. An official list of indexes and categories used to identify types of DoD CUI; aligns with DoD issuances

B. A collection of classified sample documents

C. A list of DoD personnel authorized to handle CUI

D. A glossary of acronyms

7. When must DoD CUI be controlled?

A. Indefinitely.

B. Only during records active.

C. Only during official meetings.

D. Until authorized for public release under DoD public release processes.

8. What must be ensured before sharing CUI with contractors or external partners?

A. Rely solely on the contractor's internal policies; DoD requirements do not apply to contractors.

B. Confirm need-to-know, ensure proper CUI marking and safeguarding are required by contract (flow-down).

C. Share freely as long as the contractor is trusted, regardless of need-to-know.

D. Only encryption is required, no need-to-know verification.

9. Who is responsible for determining at time of creation whether info falls into a CUI category?

A. The information owner

B. The authorized holder of the document/material

C. The DoD Component security officer

D. The FOIA office

10. What are the core components of an effective CUI program?

A. Designation, marking, safeguarding.

B. Dissemination controls, decontrol, training.

C. Designation, marking, safeguarding, dissemination controls, decontrol, training, incident reporting, and enforcement.

D. Marking, training, access authorization.

Answers

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

Explanations

1. What is the high-level message about information sharing versus controls in the CUI program?

A. The program aims to promote sharing as much as possible while maintaining required safeguarding/handling measures.

B. The program prioritizes safeguarding over sharing.

C. The program aims to completely prohibit sharing.

D. The program aims to promote sharing as much as possible while maintaining required safeguarding/handling measures.

The main idea is to enable information sharing in a controlled way. The CUI program is about letting authorized people and organizations access sensitive information when needed, but only with the proper safeguards and handling requirements in place. So the message isn't about keeping everything secret or about sharing without limits; it's about sharing as much as possible while applying the required controls—marking, access, dissemination, and safeguarding procedures—to protect the information. This balance ensures collaboration and efficiency without increasing risk of misuse or disclosure. The other options imply either no sharing, or sharing without safeguards, or sharing but with no protections, which misstate the program's purpose.

2. How is CUI incident response integrated with the broader incident handling process?

A. CUI incidents are managed separately from general incident handling.

B. There is no requirement for reporting CUI incidents.

C. The CUI incident response is integrated into the broader incident handling process to ensure prompt reporting and mitigation.

D. CUI incident response is handled exclusively by the IT department.

CUI incident response is integrated into the broader incident handling process to ensure prompt reporting and mitigation. When an incident involves Controlled Unclassified Information, it should follow the same incident response lifecycle as other major security events—identify, contain, eradicate, recover, and lessons learned—so risks are addressed quickly and with proper oversight. This integration prevents handling CUI incidents in isolation, elevating them to the right stakeholders (security operations, information assurance, legal/compliance, and program owners) and coordinating through established playbooks and communication channels. It also protects the sensitive information during investigation by maintaining appropriate access controls and chain of custody. Timely reporting aligns with policy requirements and enables rapid containment and remediation, while a unified process promotes consistency, better situational awareness, and shared lessons across the organization. Keeping CUI incidents separate or leaving reporting out would introduce delays, reduce visibility, and weaken compliance and protection of CUI.

3. Under DoD public release processes, when is DoD CUI considered controlled?

A. Until authorized for public release under DoD public release processes.

B. Indefinitely.

C. Only during maintenance.

D. Only when stored in approved devices.

DoD CUI remains protected until a formal authorization for public release is granted through the DoD public release process. The release decision is the trigger that moves information from controlled to publicly releasable; until that authorization is given, it must be safeguarded and shared only with individuals who have CUI access. Once public release is approved, the information can be disclosed to the public and is no longer treated as CUI under DoD rules. The other options don't fit because the control status isn't indefinite and isn't determined by maintenance periods or device storage.

4. What does 'dissemination controls' mean in CUI handling?

A. Destruction timing.

B. Limits on how, where, and to whom CUI can be disclosed or shared.

C. Encryption standards only.

D. Only for printing and distribution.

Dissemination controls govern who can see CUI, and how and where that information can be disclosed or shared. They set the limits on disclosures to authorized individuals, within the need-to-know for the task, and specify approved methods and channels for sharing data. This is what keeps sensitive information from being released to the wrong people or through inappropriate avenues, whether internally or with external partners. Think of it as the rulebook for sharing: it covers whether, to whom, and by what means CUI can be disclosed, not when to destroy it or only how it should be encrypted, or simply how printing and general distribution are handled. Destruction timing deals with disposing of data, encryption standards with protecting data, and printing/distribution concerns a subset of handling, whereas dissemination controls govern the broader sharing restrictions.

5. What is the primary purpose of DoD Instruction 5200.48 regarding CUI within the DoD?

A. To classify all information as top secret

B. To define encryption standards for all DoD systems

C. To establish policy and responsibilities for designation, safeguarding, marking, dissemination, decontrol, and destruction of CUI within DoD.

D. To regulate personnel security clearances across DoD

DoD Instruction 5200.48 provides a unified policy framework for handling Controlled Unclassified Information within the DoD. It sets who designates CUI, how it must be safeguarded, how it should be marked, who can receive it and how it can be disseminated, when and how the CUI designation can be removed (decontrolled), and how it must be destroyed. This ensures consistent protection of sensitive but unclassified information across the department, so access is limited to authorized personnel and handling follows standardized procedures throughout creation, transmission, storage, and disposal. The other choices don't fit because they describe functions not covered by this instruction: classifying all information as top secret isn't how CUI works (CUI is unclassified but protected); defining blanket encryption standards for all DoD systems is a separate security domain outside the core purpose of CUI designation, safeguarding, and dissemination; and regulating personnel security clearances is a different policy area unrelated to the designation and handling of CUI.

6. What is the purpose of the DoD CUI Registry?

A. An official list of indexes and categories used to identify types of DoD CUI; aligns with DoD issuances

B. A collection of classified sample documents

C. A list of DoD personnel authorized to handle CUI

D. A glossary of acronyms

The DoD CUI Registry provides an official catalog of CUI categories and the DoD issuances that define them, serving as the authoritative map for identifying and classifying DoD CUI. By listing the category names, their associated identifiers, and the governing DoD documents, it ensures consistent labeling, handling, and protection across agencies and programs. This alignment with DoD issuances makes it the go-to reference for determining which category applies to a given piece of information and what markings or controls are required. The other options don't fit the registry's purpose. It is not a collection of classified sample documents, nor a roster of personnel who may handle CUI, and it isn't simply a glossary of acronyms.

7. When must DoD CUI be controlled?

A. Indefinitely.

B. Only during records active.

C. Only during official meetings.

D. Until authorized for public release under DoD public release processes.

CUI must be controlled throughout its entire life cycle until there is an official decision to release it to the public. It stays as DoD CUI and requires safeguarding, marking, and handling from creation through storage, transmission, and dissemination, wherever it resides, until the DoD Public Release Process authorizes public release. Only after that authorization is the information no longer treated as CUI. That's why the other ideas don't fit. Releasing it indefinitely would block needed transparency; restricting control only to active records ignores that CUI can exist or be shared in drafts, backlogs, or non-active contexts; and limiting control to official meetings misses the broader handling and distribution that occur beyond meetings. The public release authorization is the point at which CUI protection ends.

8. What must be ensured before sharing CUI with contractors or external partners?

A. Rely solely on the contractor's internal policies; DoD requirements do not apply to contractors.

B. Confirm need-to-know, ensure proper CUI marking and safeguarding are required by contract (flow-down).

C. Share freely as long as the contractor is trusted, regardless of need-to-know.

D. Only encryption is required, no need-to-know verification.

Before sharing CUI with contractors or external partners, you must establish need-to-know and ensure that CUI marking and safeguarding are required by the contract and flowed down to the contractor. This makes the sharing contingent on a legitimate purpose and binds the partner to the same handling standards, so the information is protected consistently. Relying on a contractor's internal policies is not enough because DoD CUI requirements apply to all recipients, and contract flow-down enforces those protections across the whole supply chain. Trust alone does not justify access, since access should be limited to individuals who truly need the information to perform the work. Encryption is valuable, but it is not the sole requirement; without proper marking, safeguarding, and need-to-know controls, sensitive information remains at risk.

9. Who is responsible for determining at time of creation whether info falls into a CUI category?

A. The information owner

B. The authorized holder of the document/material

C. The DoD Component security officer

D. The FOIA office

The person who has direct possession and responsibility for the document or material—the authorized holder—decides and applies the CUI category at the moment of creation. This role is the one charged with ensuring the correct marking and handling instructions are attached as the information is created, using the categories defined in the CUI Registry. The information owner sets the policy and provides the guidance on what categories exist and why, but the step of actually labeling and determining the category at creation falls to the authorized holder who is responsible for the material they control. The FOIA office handles disclosure requests, not classification at creation, and the DoD Component security officer oversees the security program rather than making item-by-item determinations of CUI categories.

10. What are the core components of an effective CUI program?

A. Designation, marking, safeguarding.

B. Dissemination controls, decontrol, training.

C. Designation, marking, safeguarding, dissemination controls, decontrol, training, incident reporting, and enforcement.

D. Marking, training, access authorization.

A comprehensive CUI program relies on eight integral components that together ensure CUI is identified, protected, and managed throughout its lifecycle. Designation flags information as CUI so people know it requires protection. Marking communicates the specific handling requirements on the information itself and related materials. Safeguarding covers the physical and technical protections used to store, transmit, and process CUI. Dissemination controls limit distribution to authorized recipients and specify who may access or share it. Decontrol defines when CUI protections can be removed. Training ensures personnel understand their CUI responsibilities and how to implement procedures. Incident reporting provides a formal process to report, document, and respond to losses, compromises, or breaches. Enforcement establishes accountability and mechanisms to ensure policies are followed and corrective actions are taken when needed.

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://dodinstruction520048cui.examzify.com

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