AN INTRODUCTION TO SAFEGUARDING INFORMATION:

Mastering the Realm of CDI, CUI, and CTI

sharetru

Introduction

In a world that's increasingly interconnected and digital, information has rapidly become the most valuable asset for any organization, whether governmental, corporate, or non-profit. This global digital transformation has unlocked countless opportunities, but it has also revealed a new frontier of vulnerabilities. As we languish on the brink of this digital revolution, it becomes imperative to understand, identify, and protect certain types of critical information from threat actors. This ebook aims to enlighten its readers about the integral aspects of Covered Defense Information (CDI), Controlled Unclassified Information (CUI), and Controlled Technical Information (CTI), their protection, and the vital importance of this task in modern times.

CDI, CUI, and CTI signify different categories of data, each of which demands unique treatment for safeguarding. We explore in-depth the definition, context, and type of information that falls under each of these categories. This knowledge will enhance your ability to identify and correctly classify data, a critical step toward ensuring its protection.

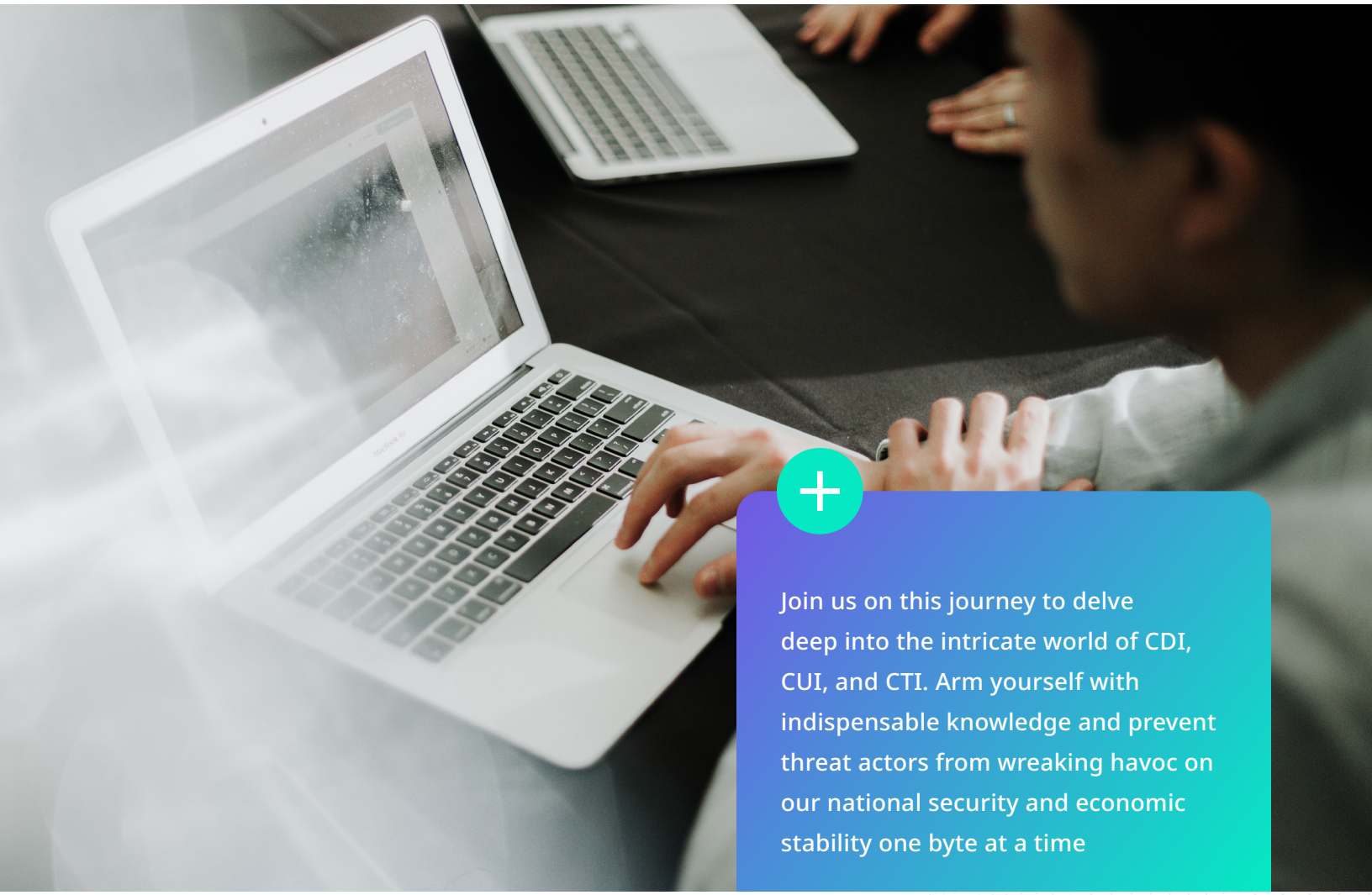
The heart of this ebook is dedicated to laying out strategies for protecting these types of information, from basic security protocols to advanced information handling and security techniques. We will unravel the veil on managing access controls, system monitoring, encryption standards, and far more. This information, coupled with real-life instances and case studies, will form a comprehensive guide, illuminating the path to stringent data protection protocols.

However, mastering the knowledge of these categories and protection techniques may not be sufficient in this escalating digital battle. The face of the adversary is constantly evolving. Nation-states, organized crime groups, and rogue individuals are continually innovating and probing soft spots in our information security fortress. They are actively working, round the clock, to breach defenses and gain unauthorized access to our valuable proprietary data. Their goal ranges from gaining economic advantages by stealing intellectual property to undermining national security or even sowing discord among societal structures.

> *"The face of the adversary is constantly evolving. Nation-states, organized crime groups, and rogue individuals ... are actively working, round the clock, to breach defenses and gain unauthorized access to our valuable proprietary data."*

The relevance of this knowledge therefore transcends individual organizations and sectors - it is of national significance.
The protection of CDI, CUI, and CTI isn't just a bureaucratic compliance exercise; it is the bulwark in the face of these persistent threats. When threat actors succeed in infiltrating our defences, the consequences can range from financial loss to a compromise of national security.

In the modern era of state-sponsored cyber-attacks, organized criminal hacking, and rampant cyber-espionage, understanding and effectively shielding CDI, CUI, and CTI becomes not just desirable, but an absolute necessity. This book will guide you through understanding these categories, identifying potential threats, and ensuring the effective protection of highly sensitive data, thereby contributing to the broader effort of safeguarding our digital landscape.



Join us on this journey to delve deep into the intricate world of CDI, CUI, and CTI. Arm yourself with indispensable knowledge and prevent threat actors from wreaking havoc on our national security and economic stability one byte at a time

What is Controlled Unclassified Information (CUI)

Controlled Unclassified Information is a category of unclassified categories designating information that requires safeguarding or dissemination controls pursuant to and consistent with applicable law, regulations, and government-wide policies.

Definition

CUI is information the U.S. government creates or possesses, or that an entity creates or possesses for or on behalf of the U.S. Government, that qualifies for one or more of the CUI categories or subcategories.

The Difference

The CUI concept is broader than the CDI concept. While CDI is specific to defense-related information, CUI encompasses a wider range of fields.

CUI includes information concerning government contracts, various types of personal data, law enforcement information, patent information, or critical infrastructure data.

CUI Basic vs CUI Specified

Controlled Unclassified Information (CUI) is a category of unclassified information that requires safeguarding or dissemination controls according to laws, regulations, and government-wide policies. CUI is divided into two subcategories: “CUI Basic” and “CUI Specified”. Here’s the difference between the two:

CUI Basic

- ”CUI Basic” is the default category for all CUI that does not fall under “CUI Specified”.
- It comprises information that necessitates safeguarding or dissemination controls according to federal laws, regulations, or government-wide policies.
- It comprises information that necessitates safeguarding or dissemination controls according to federal laws, regulations, or government-wide policies.

CUI Specified

- ”CUI Specified” is a subset of CUI where specific laws, regulations, or government-wide policies mandate stricter handling and protection requirements beyond those applicable to CUI Basic.
- The additional handling requirements for “CUI Specified” are often detailed in the underlying law, regulation, or government-wide policy, and are explicitly referenced in the CUI Registry[1].
- Examples of “CUI Specified” categories could be export-controlled information, critical infrastructure information, or certain types of personally identifiable information (PII).

Factor	CUI Basic	CUI Specified
Definition	Information that requires safeguarding or dissemination controls that are not dictated by law, regulation, or government-wide policy.	Information that requires safeguarding or dissemination controls that are dictated by law, regulation, or government-wide policy.
Safeguarding Measures	Standardized minimum controls are applied without additional requirements unless specifically prescribed.	Must follow specific safeguarding measures and handling procedures as prescribed by the law, regulation, or policy that governs the particular information.
Examples	General administrative information, certain financial records, or information covered by the Privacy Act that does not have specific handling controls outlined by statute.	Export-controlled information under the International Traffic in Arms Regulations (ITAR), information covered by the Privacy Act with specific handling controls, or health information governed by the Health Insurance Portability and Accountability Act (HIPAA).

Continued on the next page...

1. https://www.archives.gov/cui/registry/category-list

Factor	CUI Basic	CUI Specified
Marking	Marked with CUI Basic designation to indicate standard level of control.	Marked with CUI Specified designation and often with additional markings that reference the controlling law, regulation, or government-wide policy.
Access and Dissemination	Controlled within the executive branch and not released to the public without a review to determine if it can be disclosed.	Controlled both within the executive branch and when shared outside of it, including specific limitations on dissemination to foreign entities or the public.
Agency Discretion	Agencies have some discretion in implementing safeguarding measures for CUI Basic within the framework of the CUI program.	Agencies have limited discretion and must adhere to specific requirements for safeguarding and disseminating CUI Specified information.
Regulatory Framework	Governed by the overarching CUI Federal regulation, which provides a uniform policy for the treatment of CUI across the federal government.	Governed by specific laws, regulations, or government-wide policies that outline handling requirements for that specific type of information
Training and Awareness	Requires general training on handling CUI Basic information.	Requires more specialized training that covers the specific handling controls and dissemination restrictions of the CUI Specified category.

In summary, the primary difference between “CUI Basic” and “CUI Specified” is that the latter has more stringent or distinct handling and safeguarding requirements due to specific laws, regulations, or government policies that apply to that particular type of information.

What is Controlled Technical Information (CTI)

Controlled Technical Information (CTI) is technical data or computer software with military or space applications that is subject to controls on access, use, reproduction, modification, performance, display, release, disclosure, or dissemination.

Definition

Controlled Technical Information (CTI) refers to technical data or computer software that is subject to controls on access, use, reproduction, modification, performance, display, release, disclosure, or dissemination. CTI is typically associated with military or space applications and includes information that is required for the design, development, production, manufacturing, operation, maintenance, or modification of defense articles, as well as computer software directly related to defense articles.

This type of information is often critical to national defense and therefore is protected under various laws and regulations such as the International Traffic in Arms Regulations (ITAR) and the Export Administration Regulations (EAR). Access to CTI is generally restricted to authorized personnel who have a legitimate need to know, and who are usually required to undergo specialized training in handling and protecting this sensitive information. The unauthorized disclosure of CTI can have significant implications for national security and defense capabilities.

The Difference

While all three categories require protection due to their sensitive nature, CTI is specifically focused on military or space technical data, CDI broadly covers defense-related information, and CUI is an expansive category that includes a wide range of sensitive but unclassified information across various sectors.

In summary, CDI, CUI, and CTI can all overlap (as they are all types of sensitive information that need protection), but they each have distinct implications and uses. CDI relates specifically to defense-related or space program information, CUI is a broader category that consists of various types of sensitive government information, and CTI is concerned technical data or computer software with military or space applications.

Aspect	Covered Defense Information (CDI)	Controlled Unclassified Information (CUI)	Controlled Technical Information (CTI)
Definition	CDI refers to unclassified information that is specific to defense contracts and requires safeguarding or dissemination controls under law, regulations, or government-wide policies.	CUI is information that requires protection under laws and policies but is not classified. This includes a wide range of sensitive information not specific to defense.	CTI is a subset of CDI and refers specifically to military or space-related technical information requiring protection. It includes data such as research and engineering data, technical manuals, and blueprints.
Scope	Specific to defense-related information, often associated with military contracts.	Broader in scope, encompassing a wide range of sectors such as health, immigration, legal, financial, and more.	Specifically focuses on technical data related to military or space applications.
Protection Level	Requires robust safeguarding measures due to its potential impact on national security. Often involves strict access controls and handling procedures.	The level of protection varies based on the sensitivity of the information. Generally requires standard safeguarding measures.	Similar to CDI, demands high-level protection due to its potential impact on national defense and security.
Regulatory Framework	Governed by specific defense-related regulations like the Defense Federal Acquisition Regulation Supplement (DFARS).	Governed by the overarching CUI program established by Executive Order and implemented by the National Archives and Records Administration (NARA).	Governed by regulations specific to defense and military technical data, like the International Traffic in Arms Regulations (ITAR) and the Export Administration Regulations (EAR).
Access and Handling	Access is typically restricted to individuals with a legitimate need to know and often requires special training on handling CDI.	Access is controlled based on the category of CUI and the associated laws and policies. Training on handling CUI is generally required.	Access is highly restricted, often to U.S. citizens or persons with special clearance. Handling is guided by stringent regulations to prevent unauthorized dissemination.
Examples	Defense contract details, deployment plans, troop movements.	Health records, financial information, immigration statuses.	Technical specifications of military equipment, design of spacecraft, technical manuals of defense systems.

How to Protect Each Information Type

Protecting Controlled Data Information (CDI)

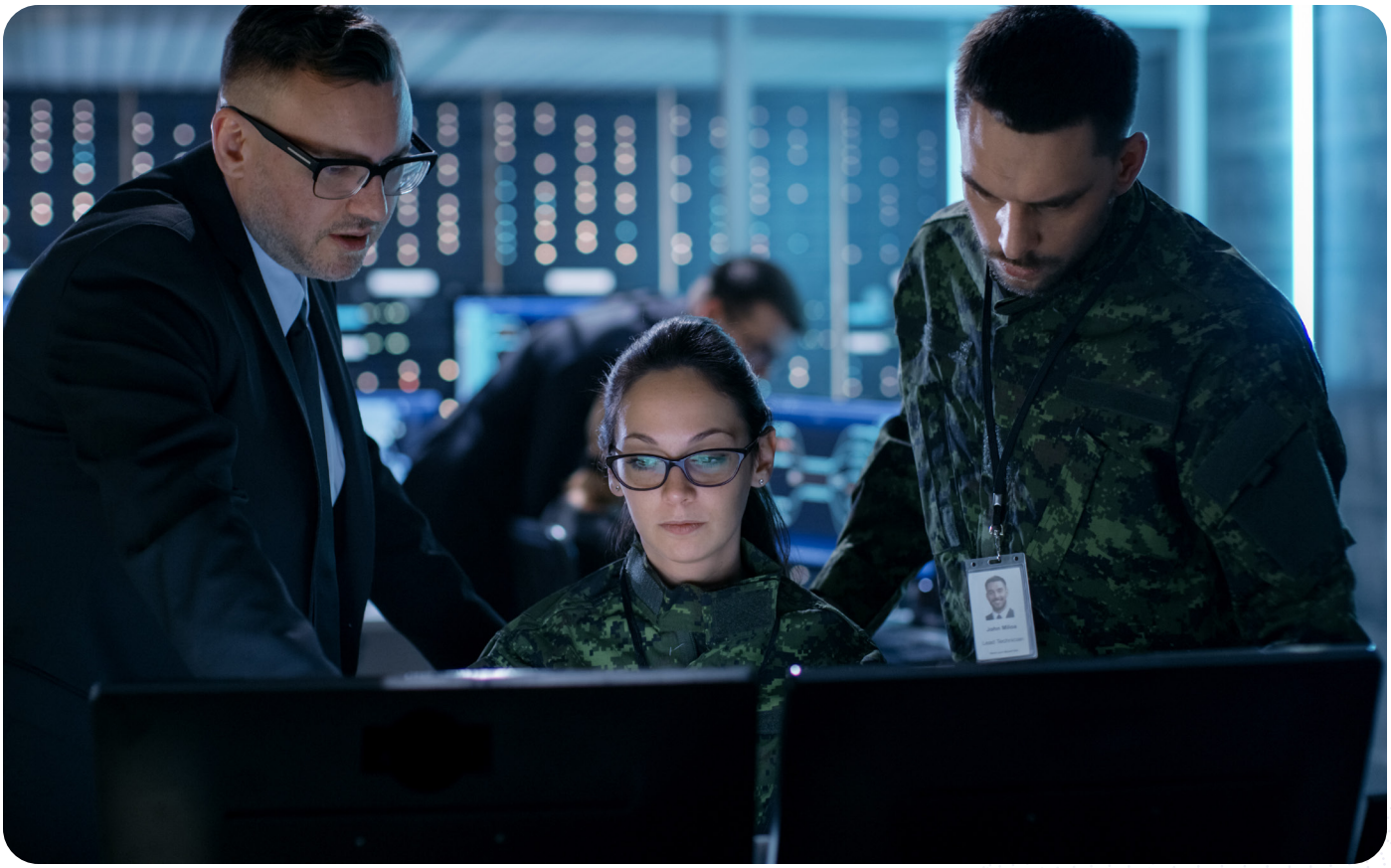
Securing CDI involves numerous strategies to get both strong physical and digital safeguards. These measures focus on preventing unauthorized access to or disclosure of the classified information. While each organization may require a distinct approach depending on their specific needs and information type, several universal best practices apply:

> *Cybersecurity is a shared responsibility and it boils down to this: in cybersecurity the more systems we secure, the more secure we all are."*
>
> - Jeh Johnson, Former United States Secretary of Homeland Security

Physical Security Measures

Physical measures to secure CDI can include:

- **Controlled Access:** Limit physical access to only authorized personnel. Implement identification procedures and controlled entry systems to prevent unauthorized personnel from gaining entry into the areas where CDI is stored.
- **Secure Storage:** Store all physical formats of CDI in locked and secure storage containers or areas when not in use.
- **Secure Transport:** If CDI needs to be transported physically, use secure methods that can prevent unauthorized access or tampering during transit.
- **Physical Monitoring:** Use security guards, surveillance cameras, and other monitoring methods to keep a close eye on areas where CDI is stored.



Technical Security Measures

Technical safeguards play an equally crucial role in CDI protection. These can include:

- **Access Control:** Limit digital access to CDI through user IDs, strong passwords, two-factor authentication, and other control methods.
- **Firewalls and Intrusion Detection Systems:** Use firewalls and intrusion detection systems to monitor and restrict incoming and outgoing network traffic based on an organization's previously established security policies.
- **Encryption:** Employ encryption to protect CDI during transmission over networks and for data at rest.
- **Regular Updates:** Regularly update all software, including operating systems and applications, to protect against potential vulnerabilities.
- **Backup and Recovery:** Maintain regular backups of CDI to protect against data loss. Ensure the backups are encrypted and securely stored.

Administrative Measures

- **Training:** Staff should receive regular training on correctly handling CDI to prevent accidental leaks or exposures.
- **Policies:** Establish clear, written policies for the handling of CDI. This should cover everything from physical to digital safeguarding measures.
- **Audit:** Regularly audit your CDI security protocols to look for potential weaknesses and areas for improvement.

Remember that the protection methods employed should be based on the sensitivity of the CDI and comply with all applicable federal laws and regulations. Always be prepared to adapt and evolve your strategies in response to new threats and challenges.

Protecting Controlled Unclassified Information (CUI)

The primary goal in securing Controlled Unclassified Information (CUI) is to ensure unauthorized access, corruption, loss, or disclosure is prevented. This requires implementing secure practices and employing the right technology, and these recommendations fall under specific categories.

This is based on Executive Order 13764, titled "Safeguarding the Controlled Unclassified Information (CUI),"issued by the U.S. government to establish a standardized framework for handling and safeguarding Controlled Unclassified Information (CUI). This order emphasizes the importance of protecting CUI and calls for the development of a uniform and consistent approach to handling this sensitive but unclassified information across federal agencies. It mandates the creation of a CUI Program to oversee the management, dissemination, and protection of CUI, ensuring that it is handled in accordance with established standards, guidelines, and safeguarding procedures. Furthermore, Executive Order 13764 encourages interagency cooperation and coordination to enhance the security and consistency of CUI handling practices across the government.

1. https://www.archives.gov/cui/registry/category-list

Here's 's a step-by-step guide to understanding and protecting CUI:

Understanding CUI

Before implementing protective measures, it's essential to know exactly what CUI is. The National Archives provides a CUI Registry[1] detailing what falls under the umbrella of CUI. Understanding this classification is necessary to ensure all relevant data is appropriately protected.

Physical Security

As with any data, the hardware hosting CUI data should be physically secure:

- **Secure Areas:** Ensure CUI is stored, accessed, and processed in secure, restricted-access physical spaces.
- **Reducing Physical Version of CUI:** Maintain the minimum physical copies of CUI and when they are not in use, secure them in a locked, protective storage area.

Technical Security

Implement robust cyber defenses to protect electronic CUI:

- **Data Access:** Implement role-based access controls ensuring only authorized personnel have access to CUI, limiting potential data exposure.
- **Encryption:** Encrypt CUI data, both at rest and transmission, to make it unreadable to unauthorized individuals.
- **Firewall and Antivirus protection:** A robust firewall and contemporary antivirus protection are critical in keeping CUI secure.
- **Monitoring and Incident Response:** By implementing proactive monitoring and creating a robust incident response plan, organizations can quickly identify and respond to potential data breaches or other security incidents.

Policy and Procedure Implementation

Developing and enforcing policies and training your team is essential:

- **Training:** Regularly train employees on the importance of CUI protection, how to handle CUI, and how to respond to potential threats.
- **Policies and Procedures:** Develop, implement, and maintain security policies involving the handling, storage, processing, and transmitting of CUI.
- **Incident Reporting:** Implement a transparent process for reporting any potential or real breaches.

> *"Amateurs hack systems, professionals hack people."*
> *- Bruce Schneier*

Assessments and Audits:

- **Compliance Audits:** Regularly audit your CUI protection practices for compliance with federal laws and Department of Defense guidelines.
- **Risk Assessments:** Conduct frequent risk assessments to identify potential vulnerabilities or threats to your stored CUI.

Remember, protecting CUI is a priority and should be treated as a continuous process, requiring regular review, updates and improvements. Understanding the nuances of CUI and the essential role it plays can ensure that protection efforts are adequately comprehensive.

Protecting Controlled Technical Information (CTI)

Protecting Controlled Technical Information (CTI) is crucial for maintaining national security and preventing unauthorized access to sensitive technical data related to defense and space applications. Effective protection strategies - Regardless of whether it's CDI, CUI, or CTI - encompass a combination of physical security measures, cybersecurity practices, personnel training, and compliance with relevant laws and regulations.

Understanding CTI

The first step to protecting CTI is understanding what constitutes CTI. Controlled Technical Information refers to technical data or computer software with military or space applications that are subject to controls on access, use, reproduction, modification, performance, display, release, disclosure, or dissemination. This encompasses a wide range of information including, but not limited to, research and engineering data, technical manuals, blueprints, and design plans for defense articles. CTI is distinct in its high sensitivity and potential impact on national security, necessitating stringent protection protocols.

Technical Security Measures

Using advanced security measures to protect your CTI systems is crucial. Here are some technical measures you can employ:

1. **Data Encryption:** Encryption should be used to ensure data confidentiality and integrity while CTI data is at rest or in transit.

2. **Network Security:** Maintain robust firewall and antivirus protections to secure your network from breaches. Implement Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) to identify and avoid potential threats, or ensure that any of your contractors have implemented these controls

3. **Access Control:** Implement strict access control measures such as two-factor authentication, or biometric verification, and ensure that only authorized personnel are granted access.

4. **Vulnerability Management:** Regularly run vulnerability assessments and penetration tests to identify and patch security gaps in your CTI systems.

Physical Security Measures

While CTI is primarily data-oriented, it's essential to incorporate physical security measures to protect the system hardware that may store or process CTI:

1. **Controlled Access:** The physical servers or systems hosting the CTI should be kept in a restricted access area with entry controlled mechanisms.

2. **Surveillance:** Monitor the premises regularly through CCTV surveillance or security personnel to mitigate the chances of physical compromise.

Policy Implementation

Policies play a crucial role in ensuring the secure handling and usage of CTI:

1. **Data Handling Policies:** Implement comprehensive procedures for how CTI is to be used, handled, shared, and discarded within the organization.

2. **Personnel Training:** Train your team regularly on the importance of CTI protection, the risks of not following the set norms, and the process to follow if any CTI breach is suspected or identified.

> *Effective protection strategies - Regardless of whether it's CDI, CUI, or CTI - encompass a combination of physical security measures, cybersecurity practices, personnel training, and compliance with relevant laws and regulations."*

Regular Audits and Compliance

1. **Compliance Audit:** Regularly audit your cybersecurity practices for compliance with relevant laws, and standards to ensure the integrity of your CTI.

2. **Risk Assessment:** Regular risk assessments help identify security gaps and prioritize improvements needed in your cyber defense.

Remember, protecting CTI requires a continuous commitment and rigorous attention to detail. By implementing advanced technical safeguards, enforcing strong security policies, and conducting consistent audits, your CTI can be secured effectively.

Exceptions to CUI, CDI, and CTI

Information categories such as Covered Defense Information (CDI), Controlled Unclassified Information (CUI), and Controlled Technical Information (CTI) are defined by specific criteria, but there are exceptions to these. Here's a breakdown:

Covered Defense Information (CDI)

1. Any information that is already lawfully available to the public without restrictions does not fall under CDI. This includes defense-related information that may have been published in open sources, such as books, academic journals, websites, or publicly accessible government documents. The key factor here is that the information must be legitimately and freely accessible without any imposed limitations on its dissemination or usage.

2. Information that does not pertain to defense services, articles, or related technical data is typically not considered CDI. For example, general administrative data, unclassified personnel records, or other non-sensitive operational data that do not directly relate to defense contracts, military operations, or defense technologies are not classified as CDI. This exception recognizes that not all information held or processed by defense entities necessarily has implications for national security or defense capabilities.

Controlled Unclassified Information (CUI)

1. CUI cannot be designated on information that is made public or is rightfully made available to the public in accordance with federal laws, regulations, or policy.

2. Information that isn't controlled by the federal agency, and isn't governed by federal information management standards or policies, is usually not considered CUI.

Controlled Technical Information (CTI)

1. Similarly to CDI, information that is lawfully available to the public without restrictions is not considered CTI. This includes technical data or software that has been published in open literature, like books, journals, or publicly accessible websites, or information that has been presented in public conferences or workshops. The key aspect here is that the information must be legitimately and lawfully available to the public without any restrictions on its dissemination.

2. Fundamental research refers to basic and applied research in science and engineering where the resulting information is ordinarily published and shared broadly within the scientific community. This type of research is typically exempt from the controls that apply to CTI, under the rationale that its open nature is beneficial for scientific progress and innovation. The exemption usually applies as long as the research is not subject to any specific access and dissemination restrictions, like proprietary information agreements or specific national security controls.

In all the cases above, the exceptions are generally centered around whether the information is already available to the public or is not directly managed by the federal agency or otherwise governed by federal information management standards or policies. Always refer to the explicit guidelines or standards of your sector or industry when classifying information.

Exercises for Understanding

Below is a list of exercises that can help you in determining if the information in question is Controlled Unclassified Information (CUI), Controlled Technical Information (CTI), or Covered Defense Information (CDI). These exercises are designed to assist you in understanding the distinctions among the three categories better.

1

Categorization Challenge: Gather various examples of information that could potentially be CUI, CTI, and CDI. Present these samples to participating team members and challenge them to categorize each set accurately. This exercise will encourage team members to review definitions and criterion for each category.

2

Case Studies: Create case studies where an organization has to manage information that might fall under CUI, CTI, or CDI. Discuss how the organization could potentially handle the data in terms of protection measures and relevant regulations. This will enable participants to link specific policies and procedures to different types of data.

3

Policy Analysis: Review your organization's existing internal policies, procedures, and guidelines related to CUI, CTI, and CDI. Conduct in-depth discussions to identify if any gaps or areas of confusion exist within these policies and how you can effectively address them to enhance the accurate classification of information.

4

Scenario-based Training: Create hypothetical scenarios where team members need to handle various types of data. In each scenario, ask participants to identify the data category (CUI, CTI, or CDI) and describe the appropriate protocols to follow.

5

Source Identification: Research specific authoritative sources related to each category, such as the National Archives for CUI[1], documents from the Department of Defense[2] for CDI, or cyber threat intelligence sharing platforms like the Cybersecurity and Infrastructure Security Agency (CISA) for CTI[3]. Present these resources to your team and discuss how they can use them to classify information more effectively.

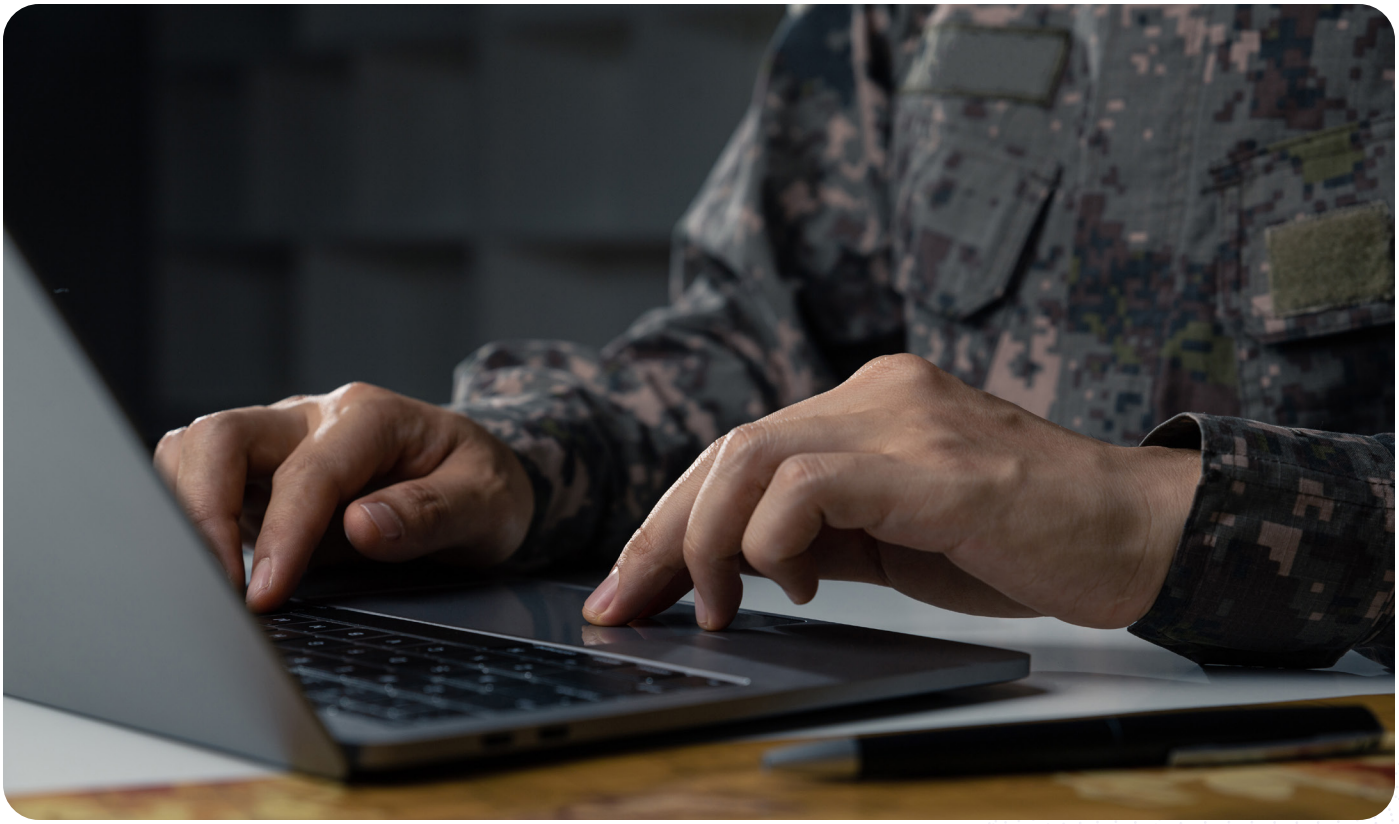
6

Reflective Quizzes: After conducting the previous exercises, give participants quizzes covering CUI, CTI, and CDI classification characteristics, protection measures, and relevant regulations to evaluate their understanding.

1. https://www.archives.gov/cui
2. https://www.dodcui.mil/
3. https://www.cisa.gov/automated-indicator-sharing-ais

Questions to Ask to Help Determine Information Type

Here's a list of questions you might ask when trying to determine if information is Classified as Controlled Unclassified Information (CUI), Covered Defense Information (CDI), or Controlled Technical Information (CTI).



1

Controlled Unclassified Information (CUI)

1. Does this information fall under any of the categories outlined in the CUI Registry[1] provided by the National Archives?

    i. Examine if the information aligns with any of the categories or subcategories identified by the National Archives and Records Administration (NARA) for CUI. This includes a broad range of topics such as privacy, financial, legal, health, critical infrastructure, and export control information.

2. Is the Information Sensitive and Requires Protection According to Laws, Regulations, or Government Policies?

    i. Determine whether the information is sensitive and requires safeguarding or dissemination controls as stipulated by federal laws, regulations, or government-wide policies. CUI does not meet the criteria for national security classification, but its unauthorized disclosure can still have adverse effects.

3. Is the Information Publicly Available or Classified?

    i. Assess if the information is publicly available without any restrictions or if it is classified. Information that is freely accessible to the public or classified under national security guidelines typically does not fall under the CUI category.

4. Does the Information Require Special Handling or Marking to Limit Access?

    i. Consider whether the information requires special handling, marking, or dissemination controls to limit access to authorized individuals. CUI often requires specific labeling and handling procedures to ensure its protection and prevent unauthorized disclosure.

1. https://www.archives.gov/cui

2

Covered Defense Information (CDI)

1. Is the Information Related to Defense Contracts or Operations?

    i. Evaluate whether the information pertains to defense contracts, operations, strategies, or activities. CDI often includes details about defense procurement, deployment plans, military operations, or other aspects directly related to national defense and security.

2. Does the Information Require Safeguarding or Dissemination Controls Under Law or Regulations?

    i. Determine if the information is subject to specific legal, regulatory, or governmental policies for safeguarding or controlled dissemination. CDI is typically protected under laws and regulations such as the Defense Federal Acquisition Regulation Supplement (DFARS) 252.204-7012.

3. Is the Information Classified or Restricted from Public Access?

    i. Assess whether the information is classified or not intended for public release. While CDI is not classified at the level of Confidential, Secret, or Top Secret, it is not publicly available and requires protection due to its sensitive nature.

4. Does the Information Include Sensitive but Unclassified Technical Data?

    i. Examine if the information includes sensitive but unclassified technical data related to defense services or articles. This can involve technical specifications, manuals, or other technical data that, while unclassified, are sensitive and require protection.

3

Controlled Technical Information (CTI)

1. Does the Information Relate to Military or Space Applications?

    i. This is the primary criterion for CTI. Ask if the information is related to the design, development, production, operation, maintenance, or modification of military equipment, systems, or software, or if it's related to space applications. This includes technical data and computer software.

2. Is the Information Subject to Controls on Access and Dissemination?

    i. Determine if there are existing restrictions on how the information can be accessed, used, reproduced, modified, performed, displayed, released, disclosed, or disseminated. CTI typically has controls to prevent unauthorized access and distribution.

3. Is the Information Publicly Available Without Restrictions?

    i. If the information is already publicly available without restrictions (for example, published in open literature or available on public websites), it generally does not qualify as CTI. CTI is typically not in the public domain.

4. Does the Information Include or Relate to Export-Controlled Technical Data?

    i. Consider if the information falls under export control regulations, such as the International Traffic in Arms Regulations (ITAR) or the Export Administration Regulations (EAR). Information that is subject to these regulations is often classified as CTI due to its sensitivity and potential impact on national security.

When you answer these questions considering the particular data you have, you can make a more accurate determination as to whether the information is CUI, CDI, or CTI.

APPENDIX

Glossary of Terms

CDI (Covered Defense Information): Unclassified information related to defense items, services, and technical data that the U.S. government requires protection for, including technical drawings, plans, models, engineering activities, specifications, and reports.

CISA (Cybersecurity and Infrastructure Security Agency): The U.S. federal agency tasked with protecting the nation's critical infrastructure from physical and cyber threats.

Compliance Audits: Systematic reviews to determine whether an organization is conducting its operations in accordance with prescribed laws, regulations, policies, and procedures.

Cryptographic Module: A set of hardware, software, firmware, or some combination thereof that implements cryptographic functions or processes, including cryptographic algorithms and, typically, key generation, encryption, and decryption.

CTI (Controlled Technical Information): Information that assists organizations in identifying, assessing, monitoring, and responding to cyber threats, including indicators of compromise and tactics, techniques, and procedures of threat actors.

CUI (Controlled Unclassified Information): Information that the U.S. government or its contractors create or possess that requires safeguarding or dissemination controls pursuant to law, regulations, and government-wide policies.

CUI Basic: The default level of CUI which requires standard safeguarding measures as outlined by the CUI program.

CUI Specified: CUI that requires specific safeguarding measures and handling procedures as dictated by law, regulation, or government-wide policy.

Data at Rest Encryption: The encryption of data that is not actively moving from device to device or network to network such as data stored on a hard drive, laptop, flash drive, or archived/stored in some other way.

Data In Transit Encryption: The encryption of data that is actively moving from one location to another, such as across the internet or through a private network.

DFARS (Defense Federal Acquisition Regulation Supplement): Regulations that provide the Department of Defense with acquisition regulations that are specific to its needs.

DoD (Department of Defense): The U.S. federal department responsible for coordinating and supervising all agencies and functions related to national security and the Armed Forces.

Encryption: The method by which information is converted into secret code that hides the information's true meaning.

Firewall: A part of a computer system or network that is designed to block unauthorized access while permitting outward communication.

HIPAA (Health Insurance Portability and Accountability Act): Legislation that provides data privacy and security provisions for safeguarding medical information.

Indicators of Compromise (IoCs): Forensic data that suggests an information security incident has occurred or is occurring.

Intrusion Detection Systems (IDS): Devices or software applications that monitor networks or systems for malicious activity or policy violations.

ITAR (International Traffic in Arms Regulations): Regulations that control the export and import of defense-related articles and services on the United States Munitions List.

Malware: Software that is specifically designed to disrupt, damage, or gain unauthorized access to a computer system.

Nation-state: A sovereign state whose citizens or subjects are relatively homogeneous in factors such as language or common descent.

NIST (National Institute of Standards and Technology): An agency of the U.S. Department of Commerce that develops technology, metrics, and standards to drive innovation and economic competitiveness.

Phishing: A cybercrime in which a target or targets are contacted by email, telephone, or text message by someone posing as a legitimate institution to lure individuals into providing sensitive data.

PII (Personally Identifiable Information): Information that can be used to identify, contact, or locate an individual, either alone or combined with other easily accessible information.

Risk Assessments: The process of identifying and analyzing potential issues that could negatively impact key business initiatives or projects.

Tactics, Techniques, and Procedures (TTPs): The patterns of activities or methods associated with a specific threat actor or group of threat actors.

Threat Actor: An individual or group that performs an action that can potentially cause harm to a computer system or organization.

Threat Intelligence Report: Documentation produced by analyzing data about current or potential attacks that threaten the security of an organization or system.

CASE STUDY EXAMPLE:

Identifying CUI, CDI, and CTI Information

You can find more case studies by downloading our case study resource guide

Scenario:

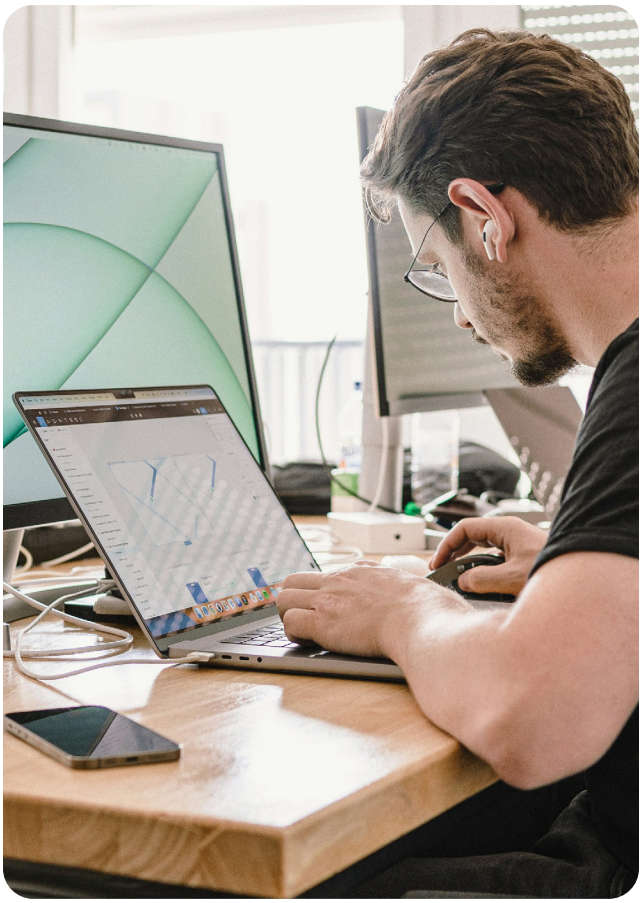
A government contractor, XYZ Technologies, is responsible for developing software for a federal agency. As part of their contract, XYZ Technologies must handle Controlled Unclassified Information (CUI), Covered Defense Information (CDI), and Critical Technical Information (CTI) in compliance with government regulations. A group of employees needs to determine whether specific information falls under the categories of CUI, CDI, or CTI to ensure proper handling and protection.

Background:

- **CUI (Controlled Unclassified Information):** CUI is information that requires safeguarding or dissemination controls in accordance with laws, regulations, or government-wide policies. It is not classified but still requires protection due to its sensitive nature.
- **CDI (Covered Defense Information):** CDI is a subset of CUI that is directly related to national security and defense. It includes sensitive information that, if disclosed, could harm national security interests.
- **CTI (Controlled Technical Information):** CTI refers to technical information related to defense systems, technologies, or operations that is critical to maintaining a military advantage. It is a subset of CDI and requires special handling and protection.

Objective:

To determine whether specific pieces of information qualify as CUI, CDI, or CTI and to understand the appropriate handling and protection requirements for each category.



Case Study Scenarios:

Scenario 1: Employee Handbook
XYZ Technologies has an employee handbook that contains guidelines on office conduct and policies. Does the content in the employee handbook fall under CUI, CDI, or CTI?

Scenario 2: Project Specification
XYZ Technologies is working on a project for the Department of Defense (DoD). The project specifications include technical details about the software being developed. Are these project specifications considered CUI, CDI, or CTI?

Scenario 3: Supplier Information
XYZ Technologies has a list of suppliers and their contact details. Is this supplier information categorized as CUI, CDI, or CTI?

Scenario 4: Encryption Algorithm
XYZ Technologies uses a proprietary encryption algorithm in its software. Is the technical information related to this encryption algorithm considered CUI, CDI, or CTI?

Scenario 5: Personnel Records
XYZ Technologies maintains records of its employees, including their names, addresses, and social security numbers. Do these personnel records fall under CUI, CDI, or CTI?

Help your employees

understand CDI, CUI, and CTI with our 5 case studies.

Download Now

Steps to Determine Classification

In each scenario, employees should follow these steps to determine the classification of information accurately. This process helps ensure compliance with government regulations and contract requirements while safeguarding sensitive data effectively.

1

In each scenario, employees should follow these steps to determine the classification of information accurately. This process helps ensure compliance with government regulations and contract requirements while safeguarding sensitive data effectively.

2

Examine the content: Analyze the content of the information in question. Consider whether it contains sensitive technical details, defense-related data, or critical information related to national security.

3

Consult with experts: Seek input from subject matter experts within the organization who are knowledgeable about the specific regulations and requirements.

4

Document the classification: Clearly classify the information as CUI, CDI, or CTI based on your analysis.

5

Implement appropriate handling and protection: Once classified, ensure that the information is handled and protected in accordance with the corresponding requirements for CUI, CDI, or CTI.

Do you need a MFTaaS partner to protect your organization's critical information and assets?

Try our risk-free 14 day trial today!

Start My Trial

Not ready to get started? Learn more about our platform now.

Learn More