

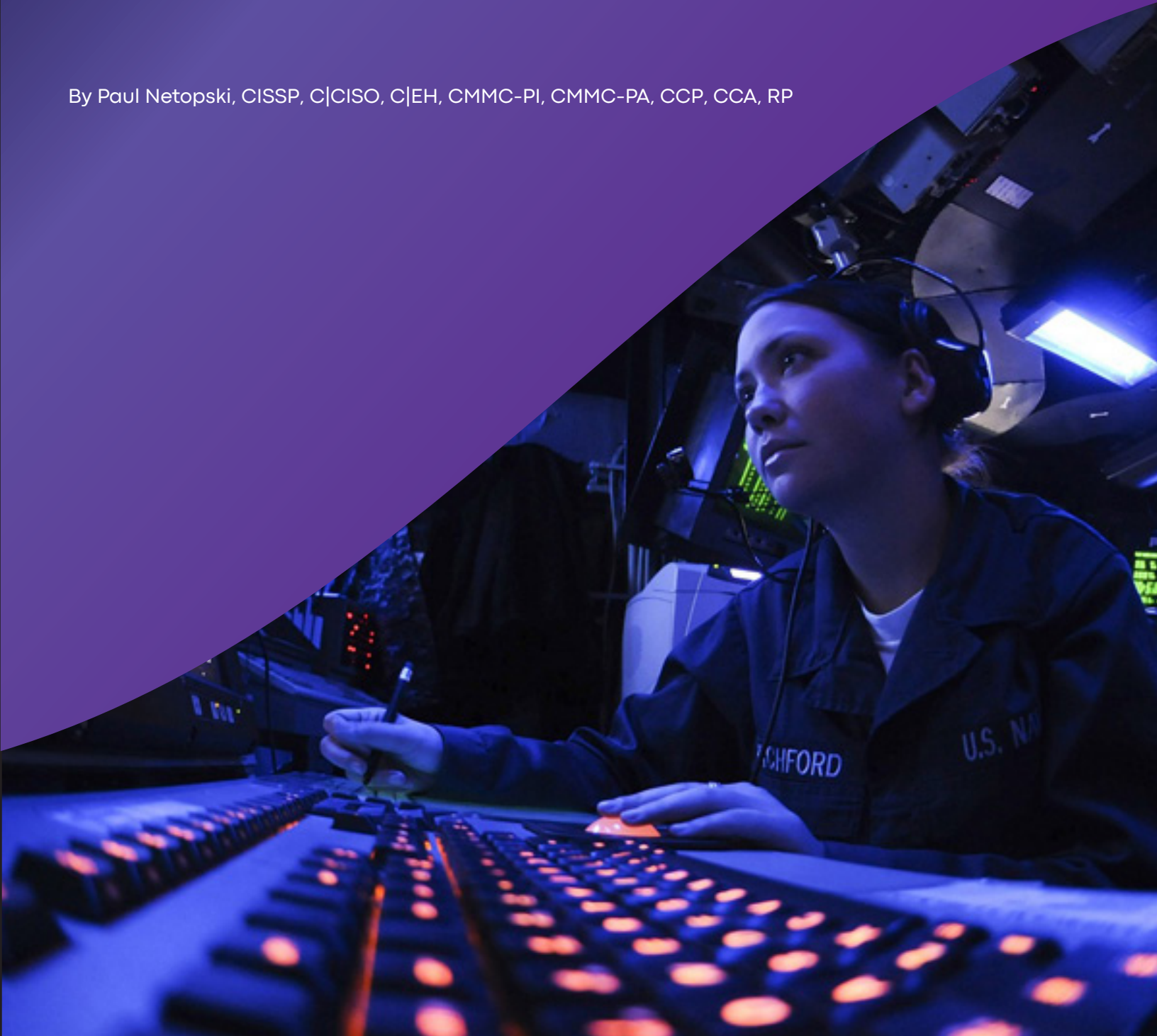


cuick trac™

Sensitive Unclassified Information

Best practices for identifying CDI, CTI and CUI, and determining how and when you need to protect it.

By Paul Netopski, CISSP, C|CISO, C|EH, CMMC-PI, CMMC-PA, CCP, CCA, RP



Executive Summary

Controlled Unclassified Information (CUI) Registry

Not all information listed in the National Archives and Records Administration (NARA) Controlled Unclassified Information (CUI) registry is CUI for your organization. The information categories are general categories for the Federal Government to follow. The information in those categories must fall under the specific codified rule to be considered CUI. When the government is issuing a contract, they must specify to the performing contractor what information will be generated under the performance of the contract that will be under the governance of the codified ruling.

Covered Defense Information (CDI)

Determining if you have Covered Defense Information (CDI) today or anticipating where CDI may reside once awarded a contract can be a challenge. Controlled Unclassified Information (CUI) is a type of CDI, so we will work on determining if CDI in your environment. We will focus on items in the list below:

- Identify requirements in the contract
- Understand what the requirements are and how they apply to your organization
- Work with your organization to understand how they plan on executed the contract (should be completed when determining if your organization will submit a proposal)
- Create diagrams to understand where data will flow in your organization

Other Considerations

Develop a scoping boundary around the technology, people and places that will process, store or transmit CDI.

If possible, segment off that technology to limit the exposure to CDI in the organization.

Apply the requirements dictated in the contract around the technology, people and locations in the scoping boundary.

Assess your organizations application of requirements using assessment criteria referenced in the requirements.

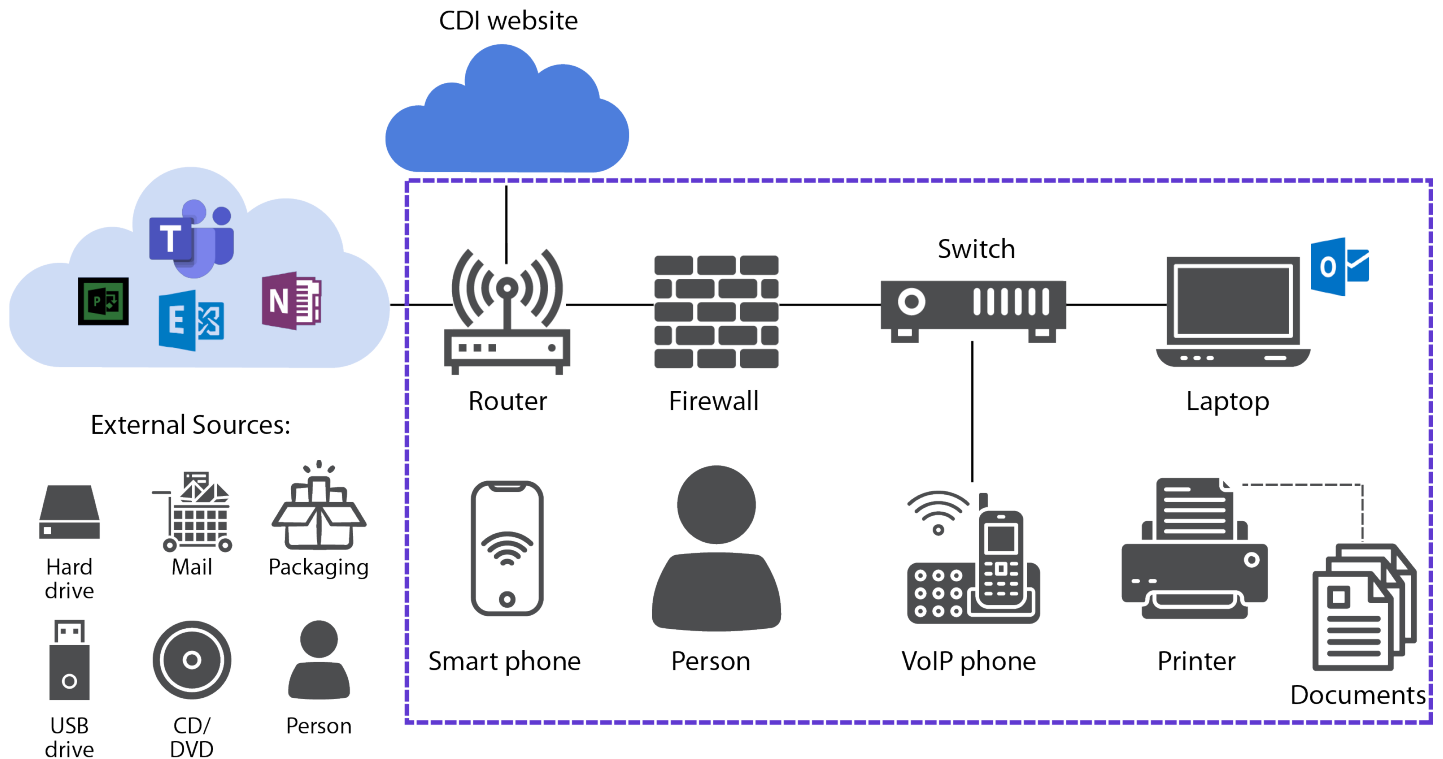
About the Author



Paul Netopski, CISSP, C|CISO, C|EH, CMMC-PI, CMMC-PA, CCP, CCA, RP

Paul Netopski is the Director of Compliance Advisory for Beryllium InfoSec and Quick Trac, and the CEO of Critical Prism Defense, LLC. For the past 20 years, he has held various space and defense industry roles in cybersecurity and information technology, and specializes in providing synchronous full lifecycle management of services for engineering and product development teams. Paul is a CMMC Provisional Instructor, Provisional Assessor, CCP, CCA and Registered Practitioner.

Simple Scoping Diagram



Covered Defense Information (CDI)

Definition from DFARS 252.204-7012

“Covered defense information” means unclassified controlled technical information or other information, as described in the Controlled Unclassified Information (CUI) Registry at <http://www.archives.gov/cui/registry/category-list.html>, that requires safeguarding or dissemination controls pursuant to and consistent with law, regulations, and Government-wide policies, and is:

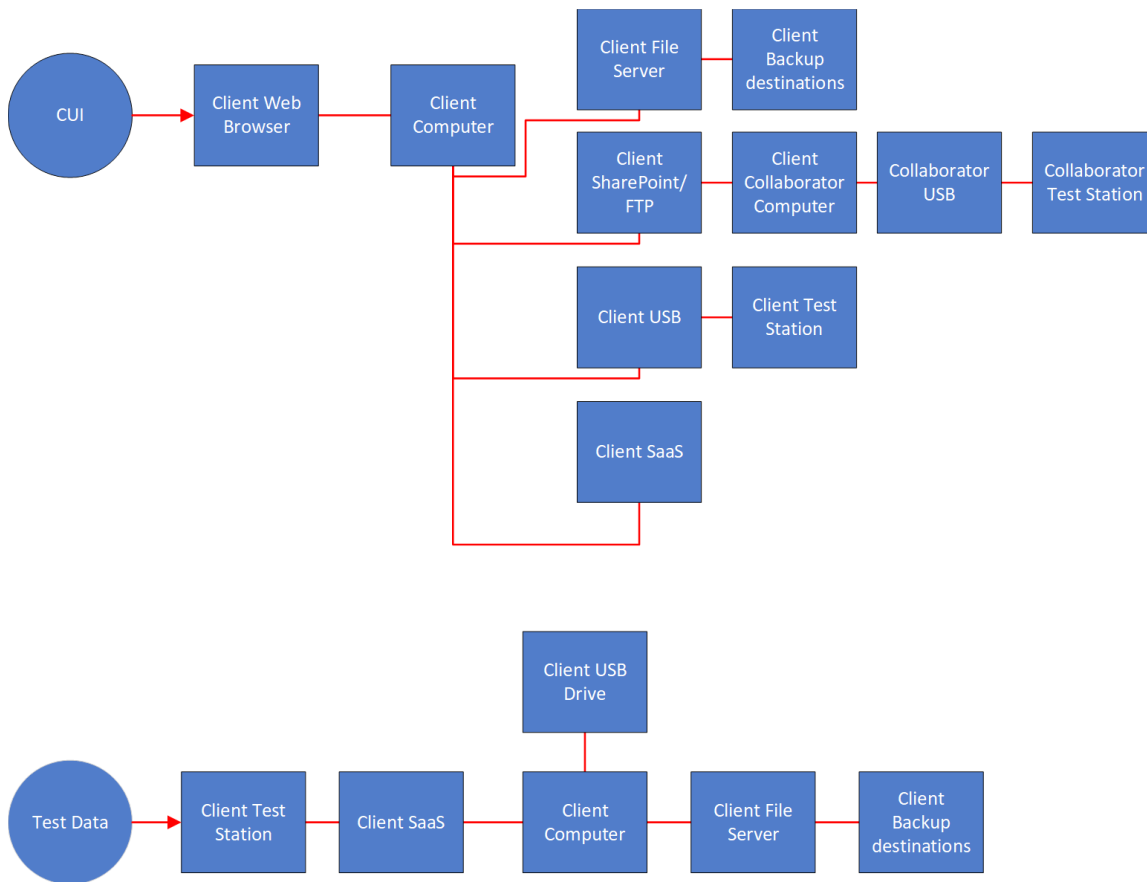
(1) Marked or otherwise identified in the contract, task order, or delivery order and provided to the contractor by or on behalf of DoD in support of the performance of the contract; or

(2) Collected, developed, received, transmitted, used, or stored by or on behalf of the contractor in support of the performance of the contract.

NARA CUI Index Groups

- Critical Infrastructure
- Defense
- Export Control
- Financial
- Immigration
- Intelligence
- International Agreements
- Law Enforcement
- Legal
- Natural and Cultural Resources
- North Atlantic Treaty Organization (NATO)
- Nuclear
- Patent
- Privacy
- Procurement and Acquisition
- Proprietary Business Information
- Provisional
- Statistical
- Tax
- Transportation

Sample Data Flow Diagram



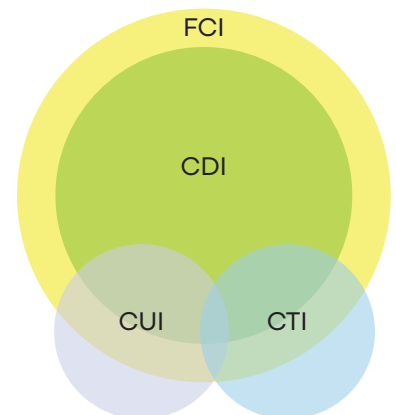
How do you get CDI in your environment?

How to determine if the information is Covered Defense Information (CDI)?

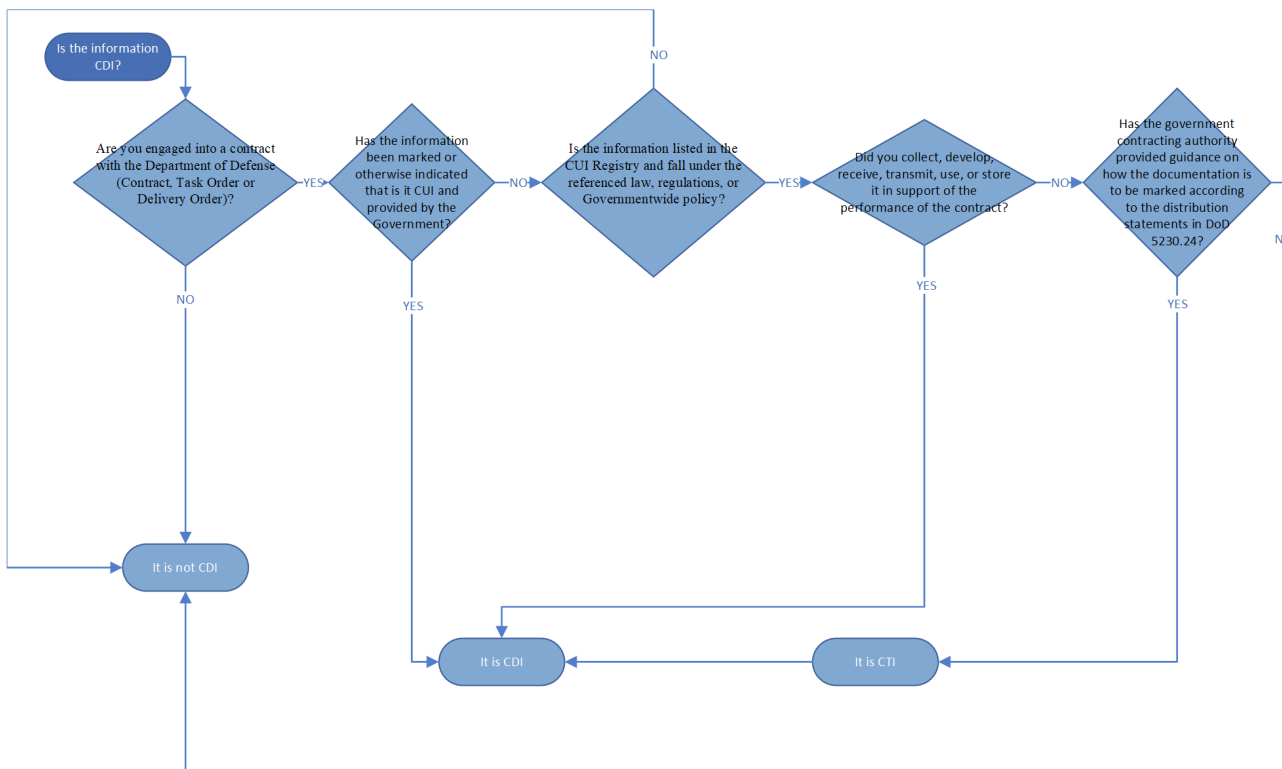
The key reference here is CDI, because it is specifically called out in DFARS 252.204-7012 and is key to identifying what information is considered CUI in your environment.

Determining how you get CDI into your environment is challenging, especially if you are trying to do it on your own. The organization should get together and talk about their overall business process flow. If your organization has a Federal business group, you may want to focus on that specific group first. Using a business process flow data collection tool to focus on specific questions during all phases of the business capture and execution process will be essential to understand how CDI may get into your environment, keeping in mind your environment includes people, technology and locations. You may receive physical CDI and not digital, so if your focus is solely on your Information Technology Systems, you will be missing the other 2/3rds of the scope.

Federal Government Sensitive
Unclassified Information
Categories (Contract Related)



CDI Determination Workflow



Q1

Does the document have a distribution statement from DoD 5230.24 Controlled Technical Information (CTI)?

Q2

Or; does the document contain other information in the CUI registry that requires safeguarding or dissemination controls pursuant to and consistent with law, regulations, and Governmentwide policies. This means, if you review the CUI Categories, select one of the specific items in the category, you will find the "Safeguarding and/or Dissemination Authority" block with a Codified requirement (x USC xxx). If you open that codified requirement, it should state specifically the information type that has to be safeguarded. There may be multiple Codified references for a CUI category. Remember NARA had to review all codified rules and categorize the references to specific data types that all government agencies could use that would be similar enough.

*If you answered yes to question #1 or #2, then continue to question #3.
If you answered no to both questions #1 and #2, it is not CDI.*

Q3

Was the information marked or otherwise identified in the contract, task order, or delivery order and provided to the contractor by or on behalf of DoD in support of the performance of the contract?

Or was the information collected, developed, received, transmitted, used, or stored by or on behalf of the contractor in support of the performance of the contract?

Following the Data

A Sample Business Process Flow document can be found on the next page. During this exercise you should be identifying how the business is receiving or sending information, such as via email, website, postal carrier or other methods. In the Business Process Flow there is a line between project award and project execution, this is because the information will not be CDI in the earlier phases before that line (in most cases), this is because in order for something to be considered CDI, it must be as part of the performance of a contract.

- **Electronic:** Electronic information may enter your environment through websites, file sharing, collaboration platforms and/or email. Your organization should develop a Data Flow Diagram which can be developed following your business process flow.

- **Paper:** Paper may enter your organization from a person, postal/shipping service, fax (yes they are still used) or even someone internally printing a digital version... people still use notebooks too.

- **Media:** Digital data that could have been retrieved from the areas identified previously could have been put onto removable media and transferred to your systems. CD, DVD, USB Data drives, or even small media devices (SD, microSD, MiniSD or others). Also remember that Camera or other smart devices could be connected to systems to transfer the information (cell phone, media players).

- **Hardware:** Your organization may be machining or integrating products which may be CDI afterwards. Maybe your organization is putting final touches on a product that is already CDI. These devices will either be made by your people and technology or received from postal/shipping sources (maybe even hand carried by the supplier or an employee).

Section 874 of the 2023 National Defense Authorization Act

SEC. 874. INCORPORATION OF CONTROLLED UNCLASSIFIED INFORMATION GUIDANCE INTO PROGRAM CLASSIFICATION GUIDES AND PROGRAM PROTECTION PLANS.

(a) UPDATES REQUIRED.—

(1) IN GENERAL.—The Secretary of Defense shall, acting through the Under Secretary of Defense for Intelligence and Security and the Under Secretary of Defense for Research and Engineering, ensure that all program classification guides (for classified programs) and all program protection plans (for unclassified programs) include guidance for the proper marking for controlled unclassified information (CUI) at their next regularly scheduled update.

(2) ELEMENTS.—Guidance under paragraph

(1) shall include the following:

(A) A requirement to use document portion markings for controlled unclassified information

(B) A process to ensure controlled unclassified information document portion markings are used properly and consistently.

(b) MONITORING OF PROGRESS.—In tracking the progress in carrying out subsection (a), the Under Secretary of Defense for Intelligence and Security and the Under Secretary of Defense for Research and Engineering shall implement a process for monitoring progress that includes the following:

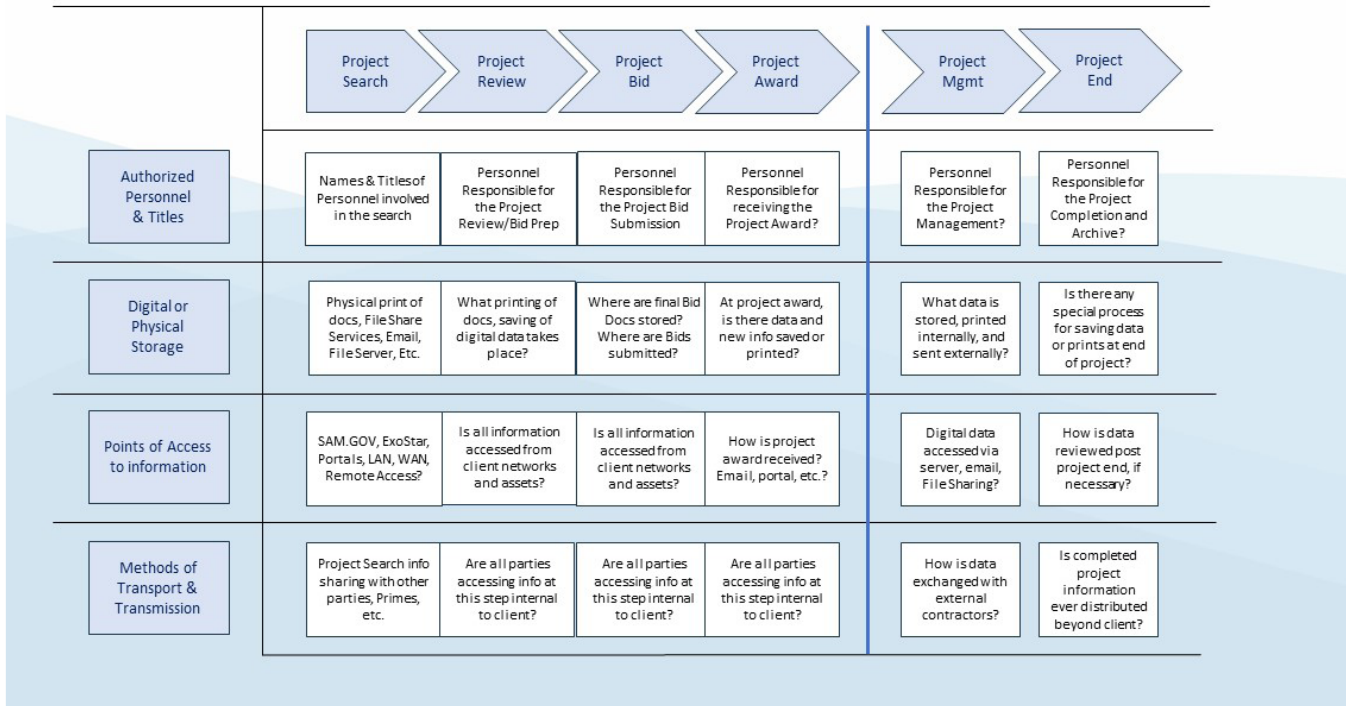
(1) Tracking of all program classification guides and program protection plans so they include document portion marking for controlled unclassified information, and the dates when controlled unclassified information guidance updates are completed.

(2) Updated training in order to ensure that all government and contractor personnel using the guides described in subsection (a)(1) receive instruction, as well as periodic spot checks, to ensure that training is sufficient and properly implemented to ensure consistent application of document portion marking guidance.

(3) A process for feedback to ensure that any identified gaps or lessons learned are incorporated into guidance and training instructions.

(c) REQUIRED COMPLETION.—The Secretary shall ensure that the updates required by subsection (a) are completed before January 1, 2029.

Business Process Flow Diagram



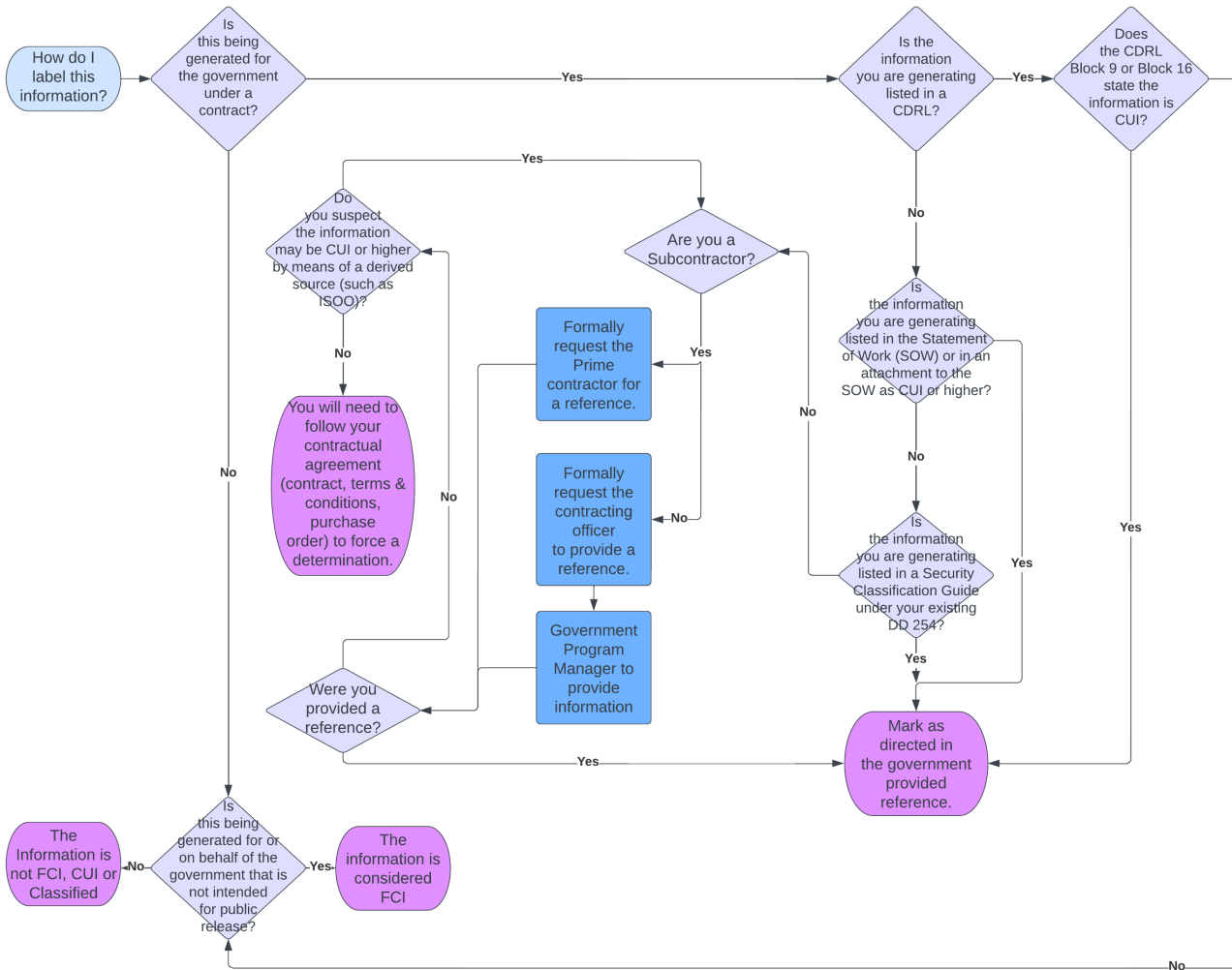
How to identify what information will be CUI, CTI, CDI?

When thinking about types of media and the way they get into your organization (or out of it) it may make it a little easier to start scoping out your environment and setting up controls to prevent the information from getting out of control. Technical controls are not the only type of controls your organization should be putting up to control the flow of CDI in the environment. Also remember that the information would only be considered CDI if it was already marked, or it is communicated to you through a contract, terms and conditions, a purchase order or other official medium stating that specific information is CDI. In a contract it should be found in one of the following locations (as communicated in DoD publications and the DFARS clauses):



- The Statement of Work (SOW) or Performance Work Statement (PWS)
- An attachment to the SOW, such as a specifications or requirements document
- SOW Contract Data Requirement List (CDRL), DD Form 1423, Block 9 or Block 16
- A Security Classification Guide (SCG)
- Program Protection Plan (PPP)

FCI or CUI Determination Workflow



CDRL: DD1423

CONTRACT DATA REQUIREMENTS LIST (1 Data Item)						Form Approved OMB No. 0704-0188 OMB Approval Expires 20221130		
The public reporting burden for this collection of information is estimated to average 110 hours per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing the burden, to the Department of Defense, Executive Services Directorate (0704-0188). Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to any penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number. Please do not return your form to the above organization. Send completed form to the Government Issuing Contracting Officer for the Contract/PR No. listed in Block E.								
A. CONTRACT LINE ITEM NO.			B. EXHIBIT		C. CATEGORY:			
					TDP <input type="checkbox"/>		TM <input type="checkbox"/>	
D. SYSTEM/ITEM			E. CONTRACT/PR NO.		F. CONTRACTOR			
1. DATA ITEM NO.	2. TITLE OF DATA ITEM				3. SUBTITLE			
4. AUTHORITY (Data Acquisition Document No.)			5. CONTRACT REFERENCE			6. REQUIRING OFFICE		
7. DD 250 REQ	9. DIST STATEMENT REQUIRED		10. FREQUENCY		12. DATE OF FIRST SUBMISSION		14. DISTRIBUTION	
							b. COPIES	
8. APP CODE			11. AS OF DATE		13. DATE OF SUBSEQUENT SUBMISSION		a. ADDRESSEE	
							Draft	
							Final	
							Reg	
							Repro	
16. REMARKS								

Controlled Technical Information (CTI)

Definition from DFARS 252.204-7012

“Controlled technical information” means technical information with military or space application that is subject to controls on the access, use, reproduction, modification, performance, display, release, disclosure, or dissemination. Controlled technical information would meet the criteria, if disseminated, for distribution statements B through F using the criteria set forth in DoD Instruction 5230.24, Distribution Statements on Technical Documents. The term does not include information that is lawfully publicly available without restrictions.

DoDi 5230.24

Ensure that the controlling DoD office that created or sponsored the work exercises its inherently governmental responsibility to determine the appropriate marking in accordance with this Instruction, Reference (j), and Volumes 2 and 4 of DoD Manual 5200.01 (Reference (l)), and that all technical documents, including research, development, engineering, test, sustainment, and logistics information, regardless of media or form, are marked correctly.

DoD distribution statement markings shall not be required on technical proposals or similar documents submitted by contractors seeking DoD funds or contracts; however, markings prescribed by applicable acquisition regulations shall apply.

Controlled Technical Information Distribution Statements

DISTRIBUTION STATEMENT A. Approved for public release: distribution is unlimited.						
DISTRIBUTION STATEMENT B. Distribution authorized to U.S. Government agencies [category] [date of determination]. Other requests for this document must be referred to [controlling DoD office].						
DISTRIBUTION STATEMENT C. Distribution authorized to U.S. Government agencies and their contractors [category] [date of determination]. Other requests for this document must be referred to [controlling DoD office].						
DISTRIBUTION STATEMENT D. Distribution authorized to Department of Defense and U.S. DoD contractors only [category] [date of determination]. Other requests for this document must be referred to [controlling DoD office].						
DISTRIBUTION STATEMENT E. Distribution authorized to DoD Components only [category] [date of determination]. Other requests for this document must be referred to [controlling DoD office].						
DISTRIBUTION STATEMENT F. Further distribution only as directed by [controlling DoD office] [date of determination] or higher DoD authority.						
REL TO. Information has been predetermined by the DoD controlling agency, in accordance with established foreign disclosure policies, to be releasable through established foreign disclosure procedures and channels, to the foreign country and international organization indicated.						
	CATEGORY	A	B	C	D	E
	PUBLIC RELEASE	X				
	CTI		X	X	X	X
	CONTRACTOR PERFORMANCE EVALUATION		X			X
	CRITICAL TECHNOLOGY		X	X	X	X

Summary

While many organizations are hoping that the 2023 NDAA Section 874 will be the savior for identifying CDI, CFI or CUI in contracts, the chances are that it will not be comprehensive enough to clearly communicate if the information is to be marked or protected as such.

The Defense Industrial Base (DIB) is contracted out to perform these services for the Federal Government because the Federal Government doesn't have the capabilities or expertise to perform it in a similar fashion. It will require DIB companies to work closely with the government contracting officers to identify the types of information being generated, at which phase and if the DIB company thinks it may fall under one of those categories. The DIB must also be prepared to defend if something should not fall under one of those categories.



REMEMBER

Open the reference in the CUI Registry category to the applicable Government Law (applicable Code of Federal Regulations) that provides details about the information that needs to be protected as CUI; it is not all information associated with that particular index group.

Protect the information

1. Review Contracts—Review your SOW, PWS, CDRL, Specifications, Purchase Orders, Terms & Condition to see what type of information is to be considered FCI, CDI, CTI or CUI
2. Business Process Flow—Understand how your business uses information, write it down.
3. Data Flow—Develop Data flow diagrams to map how your business uses information to the technology. Also look to see how it is to be shared (internal & external) to setup your boundaries.
4. What you Create—What will be created during the execution of the contract? Talk to the contract execution team, are you making code, drawings, slides, documents, spreadsheets, unprocessed data, processed data, visualizations, taking in someone else's proprietary information, etc... Create a cross reference table and determine if those types of information "may" be considered FCI, CDI, CTI, CUI. Follow the flowcharts to determine if it falls into one of the categories. Send the crossreference to your government contracting officer. It would be best to do this in the RFP phase, since it could impact workflows, costs and timelines.
5. Develop your Policies, Practices, Procedures, Processes and technical controls to protect the information following NIST SP800-171 revision 2.
6. Education and Training—Provide Education to the personnel that will be working on the project. Outline what information is sensitive and how they should be using the company resources to protect it (e.g. if you need to send the information to an external organization, use this tool and follow that standard operating procedure). Communicate with your suppliers and sub contractors.

RESOURCES

Executive Order 13556
DFARS 252.204-7012
DoD 5200.48P
DoD 5230.24
DoD CUI Program

DD Form 1423-1 (CDRL)
Developing & Using Security Classification Guides
Program Protection Plan Template (PPP)
Statement of Work Template (SOW) - MIL-STD-961
Performance Work Statement Handbook




DoD 5200.01 Volume 1—DoD Information Security Program Overview, Classification and De-classification
DoD 5200.01 Volume 2—DoD Information Security Program—Marking of Information
DoD 5200.45—Instructions for Developing Security Classification Guides
MIL-HDBK-245D DoD Handbook for Preparation of Statement of Work



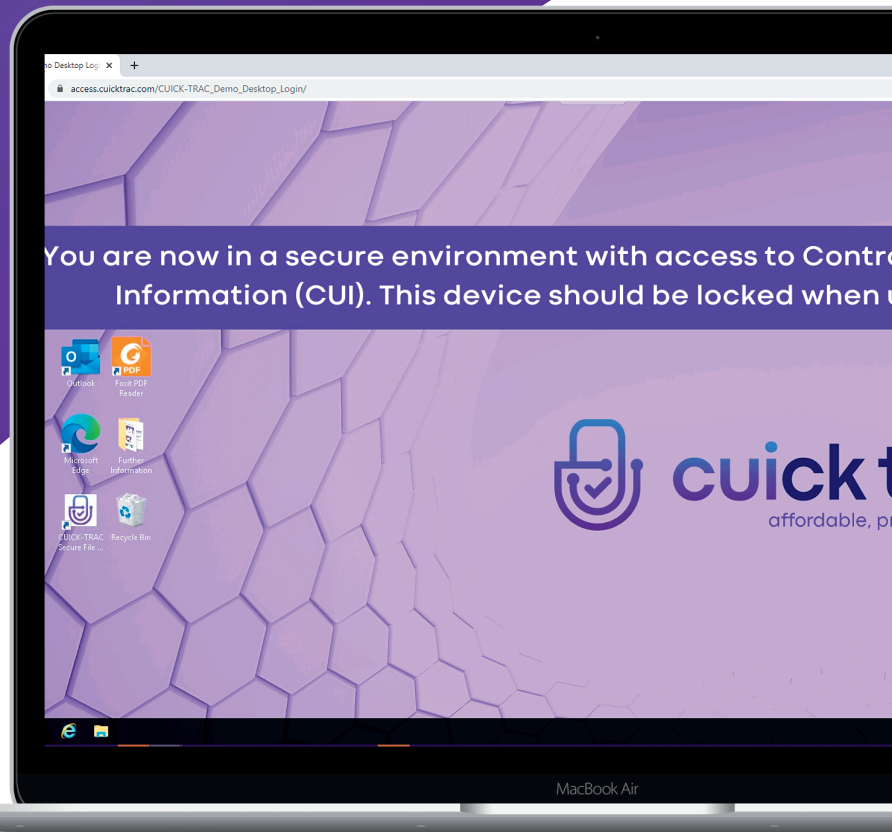
About Cuick Trac



Secure CUI in 14 days

-  Encrypted email, file sharing & storage
-  Increase your SPRS score
-  Win more contracts

Get **Cuick Trac** - a pre-configured, privately hosted CUI enclave - and be confident in your NIST 800-171 compliance program.



612-428-3008
info@cuicktrac.com
www.cuicktrac.com

cuick trac is a trademark of Beryllium InfoSec.