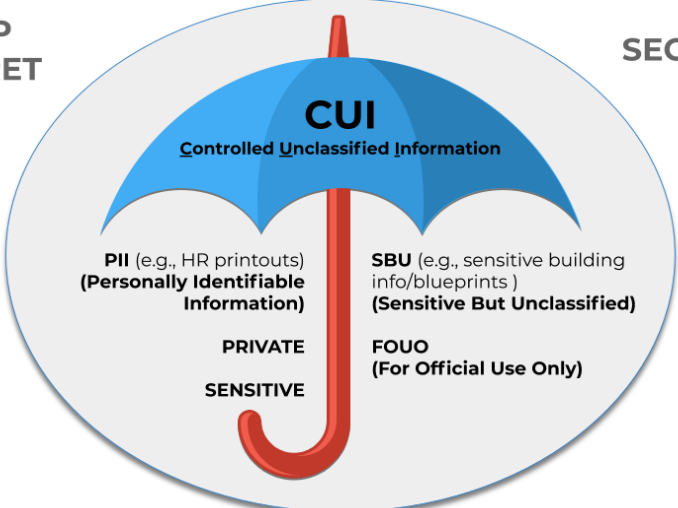


FAQs about the CUI Program

Basic Information

| | |
|--|--|
| <p>What is CUI?</p> | <p>CUI = Controlled Unclassified Information. The CUI Program standardizes common Government terminology (PII, SBU, FOUO, etc.) and practices used in protecting sensitive information such as limiting access controls based on the need to know. Watch this video which introduces various aspects of the CUI Program.</p> |
| <p>What type of info is considered CUI?</p> | <p>CUI includes certain types of information such as financial, legal, privacy, and procurement, and replaces old markings such as FOUO, SBU, PII, Private, Confidential, etc. Classified information is separate from the CUI Program.</p> <div style="text-align: center;">  </div> |
| <p>Is PII considered CUI?</p> | <p>Yes, Personally Identifiable Information (PII) falls into one of the CUI Privacy categories and will be marked and protected as CUI. The Privacy Act and other applicable Privacy policies still apply.</p> |
| <p>What about SBU, is it CUI too?</p> | <p>Sensitive But Unclassified (SBU) and other terminology will go away and be replaced with CUI terminology. Specifically, within PBS, sensitive building information that is currently considered SBU will transition to CUI (see PBS 3490.3 CHGE 1). GSA has not implemented CUI-specific markings or practices yet, but preparations are underway. So for now keep marking and protecting sensitive data, including SBU and PII, as you currently do. For more on sensitive building information, see PBS's website</p> |
| <p>Where can I learn more about CUI?</p> | <p>Information and Links to Resources can be found on the CUI InSite page (GSA internal site). NARA is the Executive Agent for the CUI Program. The CUI Registry and other information can also be found in their website: archives.gov/cui.</p> |
| <p>I keep hearing about CUI but don't see any changes yet. What's the deal?</p> | <p>GSA has not implemented CUI-specific practices yet (although many of the protections are the same as being done now, they just aren't called CUI) and some policies/guides have been updated to reflect CUI terminology. Preparations are underway to begin moving to CUI markings and procedures on July 1, 2021, but in the meantime keep marking and protecting sensitive data as you do now.</p> |
| <p>What's the difference between CUI and Controlled markings?</p> | <p>There is no difference, both are authorized CUI banner markings and either can be used as the banner marking for CUI Basic. GSA has chosen to standardize our documents by using just the letters CUI, but other agencies may use Controlled as their banner marking for CUI Basic ("Controlled" is not to be used with CUI Specified markings or when Portion marking).</p> |

| | |
|---|---|
| | Also, it is OK to add the Category abbreviation for CUI Basic, if users want to notify of the type of CUI in the document. An example of this would be CUI//PHYS. PHYS is CUI Basic so there is no "SP-" like there is in a CUI Specified category such as CUI//SP-PRVCY. |
| What's the difference between CUI Specified and CUI Basic ? | CUI Specified is a subset of CUI in which the authorizing law, regulation, or Government-wide policy contains specific handling controls that it requires, or permits agencies to use, that differ from those for CUI Basic. The CUI Registry indicates which laws, regulations, and Government-wide policies include such specific requirements. CUI Specified controls may be more stringent than, or may simply differ from, those required by CUI Basic; the distinction is that the underlying authority spells out controls for CUI Specified information and does not for CUI Basic information. CUI Basic controls apply to those aspects of CUI where the authorizing laws, regulations, and Government-wide policies do not provide any specific guidance. |
| Does GSA (or any agency) determine if CUI is Specified vs Basic? | No. The underlying authority (as listed on the CUI Registry) determines whether a category is Basic or Specified. The authorities that apply to each Category are listed in the Registry along with a link to the applicable section of that document. (Authorities = laws, regulations, or Govt-wide policies.) |
| What CUI Categories of CUI apply to GSA? | Check out this spreadsheet for an idea of the CUI Categories, Authorities, Markings, and Examples GSA is Likely to Use (internal only). |



Sharing

| | |
|---|---|
| What is a Lawful Government Purpose ? | The official definition of Lawful Government Purpose (LGP) is "any activity, mission, function, operation, or endeavor that the U.S. Government authorizes or recognizes as within the scope of its legal authorities or the legal authorities of non-executive branch entities (such as state and local law enforcement)." In other words, share only with others when the CUI will help to achieve the goals of a common project or operation between Federal agencies or others with whom there is an agreement/contract. PBS has called this "business need to know". |
| Is a Background Investigation or clearance required for someone to access CUI? | Holding CUI does not have a background investigation requirement. But many times, the people working on/with CUI will be required to have one. The types (and quantities) of information an individual works with are factors in determining public trust requirements. There are many other related factors as well, such as systems access, facility access, sensitivity of mission, and more, that can lead to the need for background investigations. But information qualifying as CUI, on its own, does not necessitate a background investigation. Refer to CIO 2180.2 GSA Rules of Behavior for Handling Personally Identifiable Information (PII) which says a background investigation may be required for PII as determined by the overall job requirements as referenced in ADM 9732.1E Personnel Security and Suitability Program Handbook and ADM 2181.1 Homeland Security Presidential Directive-12 Personal Identity Verification and Credentialing. |
| Can I send CUI in the mail ? | Yes! CUI can be sent to others via interagency mail systems, USPS, FedEx, UPS, or other commercial delivery services. Just be sure to use tracking and address it to a specific person, so you know it arrived safely. And do NOT put any CUI markings on the outside of the box or envelope. |
| How about email , how do I send CUI that way? | <ul style="list-style-type: none"> • Yes, but do not put CUI in the body of the email; it must be in an encrypted attachment. • When sending an email, the banner marking must appear at the top portion of the email, kind of like a heading. • You can add "Contains CUI" at the end of the subject line to alert recipients that CUI is present in the email. |

| | |
|--|---|
| | When forwarding or responding to email containing CUI, copy the banner markings and paste them at the top of the new email. |
| How can I share CUI with someone who has a need to know the information? | There are a number of ways to share CUI between agencies or with vendors who have a Lawful Government Purpose: <ul style="list-style-type: none"> - Encrypt the file and email it to the person, then share the password in a separate email or over the phone; - Have the recipient get a GACA account, then share the doc via a limited-access Google Drive folder; or - Use Secure File Transfer Protocol (SFTP). |
| Will FIPS-compliant WinZip ever be available on laptops (vs. thru Citrix VDI) | Unfortunately, probably not. GSA workstations are not using the Windows FIPS 140-2 validated cryptographic modules because that would encrypt traffic from end to end on Workstations. Without turning on the Windows registry flag, Winzip is only FIPS 197 certified using their own internal libraries. Basically, when turning both encryption modules on the local Windows workstations creates a system conflict in those modules. This conflict will often either lock the system up, or not allow the application to run at all. It works in Citrix because the app is installed as a stand-alone application in the virtual environment such that the cryptographic registry keys do not cause any conflict with the Windows keys. |
| Can we store CUI on a Google Site ? | Google Workspace is currently FedRAMP-authorized at the moderate level, and Sites is included in Google Workspace along with Gmail, Calendar, Meet, Chat, Drive, Docs, Sheets, Slides, Forms. So, Google Sites may be used to store CUI as long as access is limited to those with a Lawful Government Purpose. |
| Can we discuss CUI via Google Meet ? | Google says : "All data in Meet is encrypted in transit by default between the client and Google for video meetings on a web browser, on the Meet Android and Apple® iOS® apps, and in meeting rooms with Google meeting room hardware. Meet recordings stored in Google Drive are encrypted at rest by default." So yes, CUI discussions can be held over Meet, just ensure everyone in the meeting has a Lawful Government Purpose to participate and that unauthorized individuals cannot overhear conversations discussing CUI (32 CFR 2002.14). |

Marking and Coversheets

| | |
|--|--|
| Where can I get more details about Marking CUI? | See NARA's Marking Handbook . |
| We have a ton of papers in a locked file cabinet that are marked SBU. They are only kept for historical purposes. Do we have to re-mark all of them as CUI? | No, legacy documents do not have to be marked as CUI unless/until they are made "active" again. They must remain protected though and cannot be shared with other agencies with old markings. If the papers are used again they must be reviewed to see if they qualify as CUI and if so, the applicable CUI markings must be applied. |
| Can I get permission to not have to mark my very long document? | Yes. Waivers may be granted to marking CUI while it remains within GSA control (CUI is not to be shared outside of GSA unless properly marked). The information still needs to be protected according to CUI requirements. Waivers may be requested by emailing cui@gsa.gov and can be granted when: <ol style="list-style-type: none"> a) it is impractical to individually mark CUI due to quantity or nature of the information (e.g., forms, blueprints, etc.). b) following proper procedures would cause an unacceptable delay due to the urgency of the situation. Also see the Waivers to Marking CUI page and the questions below about CUI coversheets as an alternative. |
| How do I deal with sharing CUI when it's under a marking waiver ? | When a limited waiver for marking CUI has been issued and the information remains under the control of the agency, CUI does not need to be marked. When the information is shared with outside entities the CUI must be marked or identified in accordance with the CUI Program. |

| | |
|--|---|
| <p>How do you navigate a situation where you feel you have CUI but it hasn't been marked appropriately?</p> | <p>Questions regarding the status of CUI should be directed to the originator of the information or the contracting activity. This is why it is required to include information about the designating agency on the first page of a CUI document. Understand that agencies are at different stages of implementation so there will be a period where some agencies are already marking, and others aren't yet.</p> |
| <p>What is the mechanism for removing markings or lifting restrictions on documents if/when the restriction has expired or no longer applies?</p> | <p>CUI Markings can be removed (or stuck through) when the information has been decontrolled. Decontrolling occurs when an authorized holder, consistent with 32 CFR 2002 and the CUI Registry, removes safeguarding or dissemination controls from CUI that no longer require such controls. Decontrol may occur automatically or through agency action.</p> |
| <p>How do you mark databases or applications as containing CUI?</p> | <p>For databases or applications, splash screens or banner markings on each screen can be used to satisfy the marking and identification requirements of the CUI Program. Outputs from the system can also be modified to automatically apply markings upon printing or downloading from the application. If not applied automatically, the person who prints must apply the banner marking to each page. A CUI coversheet may be used to protect the information if it is excessively burdensome to mark every page but be sure to protect the information and keep it locked up when not in use.</p> |
| <p>What's the deal with CUI coversheets?</p> | <p>A CUI cover sheet may be used instead of markings when it is deemed impractical to individually mark each page due to its quantity, nature, or when a limited CUI marking waiver has been granted. The cover sheet should have written on it any CUI Specified Categories, limited dissemination controls, or requirements called for by underlying CUI authorities. Using both CUI Banner Markings and the CUI cover sheet in order to protect CUI is a best practice.</p> <p>The CUI cover sheet (Standard Form 901) is available to download from NARA's page: https://www.archives.gov/cui/additional-tools or through GSA's Forms Library. It can be printed in color or in black and white.</p>  |
| <p>How about marking external drives?</p> | <p>SF 902 and 903 can be used to label hard drives or USBs (media) that contain CUI. They can be ordered from GSA Advantage.</p>  |
| <p>Does CUI have to have Portion Markings like Classified documents do?</p> | <p>Portion marking is optional for CUI and UUI (Unclassified Uncontrolled Information). Some agencies may require it but GSA does not. The benefit to using it is if there are just a few paragraphs that contain CUI and the document is portion marked you can remove those paragraphs so that the document no longer requires CUI protections.</p> |

Safeguarding

| | |
|--|---|
| <p>What should I do with CUI while teleworking?</p> | <p>- Don't store CUI on personal computers or use personal email accounts to store or transmit CUI.</p> |
|--|---|

| | |
|--|--|
| | <ul style="list-style-type: none"> - Only use GSA approved virtual systems. - Don't print CUI if at all possible. If you have to print, protect the information until you return to the office and can destroy it properly. - Keep CUI protected at all times. Store it in a locked cabinet when not in use. |
| If a document is marked CUI//SP-PRVCY//Fed Only, do you still have to encrypt or password protect the document? | Yes. CUI must be encrypted in transit regardless of the marking or limited distribution. |
| What are the storage requirements for CUI in hard copy form (paper, disk, media)? Does it have to be stored in a locked container, locked in an office cabinet, etc. or can it be left on a desktop overnight in a locked office? | Hard copy CUI must be stored in an area or container that prevents unauthorized access. CUI may be stored in a controlled environment -- any area or space an authorized holder deems to have adequate physical or procedural controls (e.g., barriers or managed access controls) to protect CUI from unauthorized access or disclosure. Please see NARA's Controlled Environments video for additional guidance. |

Contracts/Contractors

| | |
|--|--|
| How do we deal with CUI in contracts ? | <p>A FAR case is under development that will be used to standardize the way Executive branch agencies convey safeguarding guidance for CUI. This FAR case may include a standard form that is intended to consolidate where contract related CUI requirements are conveyed. Once the FAR is finalized, all new contracts that deal with CUI will need to follow its requirements, and contractors will then be required to take the applicable agency's CUI training.</p> <p>Any information received or created as part of a current or previous contract should be protected in accordance with the terms of the contract under which it was received or created. As agencies implement, CUI requirements should be added to existing and new contracts as needed.</p> |
| For contracts, should the contracting officer tell the contractor what is CUI and how it should be marked? | Yes, that is the goal. However, as agencies are still in the process of implementing the CUI program, be sure to follow any existing requirements directing the marking or protection of unclassified information. Under the new Federal Acquisition Regulation (FAR), a standard form is being contemplated that will require this level of granularity in all contracts where CUI is involved. See 2017-016 near the end of this doc for status on the FAR Case. |
| If a contractor develops CUI under a contract (i.e. a report or deliverable submitted under the contract) does the contractor decide the marking or does the contractor ask the contracting officer to provide the category and correct marking? | Contracting authorities should provide guidance on how CUI should be marked in association with contracts. CUI Markings should align to the marking requirements found on the CUI Registry . |

Destruction

| | |
|---|---|
| Can I use any paper shredder in my office or at home to destroy CUI? | No, CUI must be destroyed in a manner that makes it "unreadable, indecipherable, and irrecoverable", specifically to 1mm x 5mm particles. Best practice is not to print. If printing is required, destroy paper in a compliant shredder, place it in a CUI-marked locked bin, or if you have to print at home, return it to an office that can destroy it properly. See NIST SP 800-88 and CUI Notice 2019-03 . |
|---|---|

| | |
|---|--|
| Does my office have a compliant shredder ? | GSA is looking at existing shredders in CO and in the ROBs and will either purchase more compliant shredders or continue to engage with shredding companies. If companies are used, there will be an agreement in place to ensure the company protects the papers in transit and destroys them to the requirements of the CUI Program. There will also be locked bins marked specifically for CUI as a place to collect papers until they can be destroyed properly. |
|---|--|

Incident Reporting

| | |
|--|--|
| What do I do if I find or receive CUI that's not properly protected , is sent to the wrong person, or something else seems amiss? | Generally, all concerns about CUI being misused or unprotected should be reported to the GSA IT Service Desk. They will gather information and work with GSA IT's incident response team to follow up and take any needed action. If the CUI that's mishandled is PII, there are specific additional requirements that must be met, which the IR Team and the Privacy Office will deal with. |
|--|--|

Other Topics

| | |
|---|---|
| Are there special Record Retention issues or timeframes specific to CUI? | No. Records retention issues/timeframes are not impacted by a document's status as CUI. Probably most official documents with CUI are considered records, but copies or working versions may not be official records. Check with your organization's records specialist or email Records@gsa.gov for more information. |
|---|---|