**CMMC DOCUMENT TEMPLATE**

# Foreword

## Introduction To The CMMC-AB

Fill in text here

## Disclaimer

Copyright 2020 CMMC-AB.

This material is based upon work funded and supported by the Department of Defense under Contract No. FA8702-15-D-0002 with Carnegie Mellon University (CMU) for the operation of the Software Engineering Institute (SEI), a federally-funded research and development center and under Contract No. HQ0034-13-D-0003 and Contract No. N00024-13-D-6400 with The Johns Hopkins University Applied Physics Laboratory LLC, a University Affiliated Research Center.

The view, opinions and/or findings contained in this material are those of the author(s) and should not be construed as an official U.S. Government position, policy or decision, unless designated by other documentation.

NO WARRANTY. THIS MATERIAL IS FURNISHED ON AN "AS-IS" BASIS. CMMC-AB MAKES NO WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, AS TO ANY MATTER INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR PURPOSE OR MERCHANTABILITY, EXCLUSIVITY or RESULTS OBTAINED FROM USE OF THE MATERIAL NOR ANY WARRANTY OF ANY KIND WITH RESPECT TO FREEDOM FROM PATENT, TRADEMARK or COPYRIGHT INFRINGEMENT.

**Table of Contents**

[Foreword 2](#_Toc43130687)

[Introduction To The CMMC-AB 2](#_Toc43130688)

[Disclaimer 2](#_Toc43130689)

[Key Terminology 4](#_Toc43130690)

[Level 1 Heading 7](#_Toc43130691)

[Level 2 Heading 7](#_Toc43130692)

[Level 3 Heading 7](#_Toc43130693)

[Appendix XX – Change Log 8](#_Toc43130694)

[Revision History 8](#_Toc43130695)

[Summary of Version Changes In Current Version 8](#_Toc43130696)

# Key Terminology

While it is the responsibility of the OSC to be fully aware of and compliant with all applicable statutory, regulatory and contractual obligations, the CMMC-AB wants OSC to be clear on the following key terminology:

**Agreements / Arrangements**[[1]](#footnote-2)

Agreements and arrangements are any vehicle that sets out specific CUI handling requirements for contractors and other information-sharing partners when the arrangement with the other party involves CUI. Agreements and arrangements include, but are not limited to, contracts, grants, licenses, certificates, memoranda of When disseminating or sharing CUI with non-executive branch entities, agencies should enter into written agreement/arrangement or understanding and information-sharing agreements or arrangements. agreements or arrangements that include CUI provisions whenever feasible (see §2002.16(a)(5) and (6) for details). When sharing information with foreign entities, agencies should enter agreements or arrangements when feasible (see §2002.16(a)(5)(iii) and (a)(6) for details).

**Authorized Holder**[[2]](#footnote-3)

Authorized holder is an individual, agency organization or group of users that is permitted to designate or handle CUI, in accordance with this part.

**Controlled Environment (FCI/CUI environment)**[[3]](#footnote-4)

Controlled environment is any area or space an authorized holder deems to have adequate physical or procedural controls (e.g., barriers or managed access controls) to protect FCI/CUI from unauthorized access or disclosure.

**Controlled Unclassified Information (CUI)**[[4]](#footnote-5)

The [**CUI Registry**](https://www.archives.gov/cui) is the authoritative source for defining CUI.

**Disseminating**[[5]](#footnote-6)

Disseminating occurs when authorized holders provide access, transmit or transfer CUI to other authorized holders through any means, whether internal or external to an agency.

**Document**[[6]](#footnote-7)

Document means any tangible thing which constitutes or contains information and means the original and any copies (whether different from the originals because of notes made on such copies or otherwise) of all writings of every kind and description over which an agency has authority, whether inscribed by hand or by mechanical, facsimile, electronic, magnetic, microfilm, photographic or other means, as well as phonic or visual reproductions or oral statements, conversations or events and including, but not limited to: Correspondence, email, notes, reports, papers, files, manuals, books, pamphlets, periodicals, letters, memoranda, notations, messages, telegrams, cables, facsimiles, records, studies, working papers, accounting papers, contracts, licenses, certificates, grants, agreements, computer disks, computer tapes, telephone logs, computer mail, computer printouts, worksheets, sent or received communications of any kind, teletype messages, agreements, diary entries, calendars and journals, printouts, drafts, tables, compilations, tabulations, recommendations, accounts, work papers, summaries, address books, other records and recordings or transcriptions of conferences, meetings, visits, interviews, discussions or telephone conversations, charts, graphs, indexes, tapes, minutes, contracts, leases, invoices, records of purchase or sale correspondence, electronic or other transcription of taping of personal conversations or conferences and any written, printed, typed, punched, taped, filmed or graphic matter however produced or reproduced. Document also includes the file, folder, exhibits and containers, the labels on them and any metadata, associated with each original or copy. Document also includes voice records, film, tapes, video tapes, email, personal computer files, electronic matter and other data compilations from which information can be obtained, including materials used in data processing.

**Due Diligence[[7]](#footnote-8)**

Due diligence the care that a reasonable person exercises to avoid harm to other persons or their property. This is a subjective benchmark to determine if an organization’s actions were sufficient enough to avoid harm. Specific to the CMMC, evidence of due diligence includes, but is not limited to:

* Documented policies, standards, and procedures;
* Developing a security-focused, multi-year business plan (e.g., roadmap) and resourcing it to achieve its goals;
* Verifying the scope of a vulnerability assessment or penetration test to ensure it is correct;
* Risk assessment of a potential vendor or other third-party; and
* Criminal background checks as a pre-requisite step in hiring decisions.

**Due Care[[8]](#footnote-9)**

Due care is the care that an ordinarily reasonable and prudent person would use under the same or similar circumstances. This is a subjective benchmark to determine whether an organization was negligent in its duty to perform its applicable statuary, regulatory and/or contractual obligations. Specific to the CMMC, evidence of due care includes, but is not limited to:

* Identifying and assigning controls to address applicable statutory, regulatory, and contractual obligations;
* Conducting ongoing maintenance (e.g., patching operations);
* Maintaining situational awareness (e.g., log reviews);
* Performing periodic risk assessments;
* Periodically reviewing permissions and ensuring only users with legitimate business needs have access;
* Performing security awareness campaigns; and
* Conducting incident response tests to validate response plans are viable.

**Federal Contract Information (FCI)[[9]](#footnote-10)**

FCI means information, not intended for public release, that is provided by or generated for the U.S. Government under a contract to develop or deliver a product or service to the U.S. Government, but not including information provided by the U.S. Government to the public (such as on public Web sites) or simple transactional information, such as necessary to process payments.

**Foreign Entity**[[10]](#footnote-11)

Foreign entity is a foreign government, an international organization of governments or any element thereof, an international or foreign public or judicial body or an international or foreign private or non-governmental organization.

**Handling**[[11]](#footnote-12)

Handling is any use of CUI, including but not limited to marking, safeguarding, transporting, disseminating, re-using and disposing of the information.

**Mechanism(s)**

A mechanism is flexible term to describe an established process, which can involve people, processes and/or technology:

* A technology-specific solution (e.g., antimalware, firewall, FIM, IPS, MFA, etc.);
* A manual procedure that an individual performs; or
* An administrative solution (e.g., acceptable use policy, human reviews, Non-Disclosure Agreements, etc.).

By using the term “mechanisms exist to…” in assessment criteria for CMMC practices, it provides flexibility for the OSC to define what is most appropriate for its unique business practices. For example, more mature organizations tend to automate their security solutions and prefer technology-specific solutions, where less mature organizations tend to rely on manual procedures or administrative solutions.

**Misuse of CUI**[[12]](#footnote-13)

Misuse of CUI occurs when someone uses CUI in a manner not in accordance with the policy contained in the Order, this part, the CUI Registry, agency CUI policy or the applicable laws, regulations and Governmentwide policies that govern the affected information. This may include intentional violations or unintentional errors in safeguarding or disseminating CUI. This may also include designating or marking information as CUI when it does not qualify as CUI.

**Unauthorized Disclosure**[[13]](#footnote-14)

Unauthorized disclosure occurs when an authorized holder of CUI intentionally or unintentionally discloses CUI without a lawful Government purpose, in violation of restrictions imposed by safeguarding or dissemination controls or contrary to limited dissemination controls.

**Working Papers (Drafts)**[[14]](#footnote-15)

Working papers are documents or materials, regardless of form, that an agency or user expects to revise prior to creating a finished product.

# Level 1 Heading

## Level 2 Heading

Text

### Level 3 Heading

Text

#### Level 4 Heading

Text

# Appendix XX – Change Log

## Revision History

|  |  |  |
| --- | --- | --- |
| **Revision #** | **Change(s)** | **Published Date** |
| 1.0 | Initial release | xxxx |

## Summary of Version Changes In Current Version

|  |  |
| --- | --- |
| **Change** | **Description of Change(s)** |
| 0 | Initial release (no change) |

1. 32CFR §2002(c) - <https://www.govinfo.gov/content/pkg/CFR-2017-title32-vol6/pdf/CFR-2017-title32-vol6-part2002.pdf> [↑](#footnote-ref-2)
2. 32CFR §2002(d) - <https://www.govinfo.gov/content/pkg/CFR-2017-title32-vol6/pdf/CFR-2017-title32-vol6-part2002.pdf> [↑](#footnote-ref-3)
3. 32CFR §2002(f) - <https://www.govinfo.gov/content/pkg/CFR-2017-title32-vol6/pdf/CFR-2017-title32-vol6-part2002.pdf> [↑](#footnote-ref-4)
4. NARA CUI Registry - <https://www.archives.gov/cui> [↑](#footnote-ref-5)
5. 32CFR §2002(v) - <https://www.govinfo.gov/content/pkg/CFR-2017-title32-vol6/pdf/CFR-2017-title32-vol6-part2002.pdf> [↑](#footnote-ref-6)
6. 32CFR §2002(w) - <https://www.govinfo.gov/content/pkg/CFR-2017-title32-vol6/pdf/CFR-2017-title32-vol6-part2002.pdf> [↑](#footnote-ref-7)
7. <https://www.merriam-webster.com/dictionary/due%20diligence> [↑](#footnote-ref-8)
8. <https://www.merriam-webster.com/legal/due%20care> [↑](#footnote-ref-9)
9. <https://www.federalregister.gov/documents/2016/05/16/2016-11001/federal-acquisition-regulation-basic-safeguarding-of-contractor-information-systems> [↑](#footnote-ref-10)
10. 32CFR §2002(y) - <https://www.govinfo.gov/content/pkg/CFR-2017-title32-vol6/pdf/CFR-2017-title32-vol6-part2002.pdf> [↑](#footnote-ref-11)
11. 32CFR §2002(aa) - <https://www.govinfo.gov/content/pkg/CFR-2017-title32-vol6/pdf/CFR-2017-title32-vol6-part2002.pdf> [↑](#footnote-ref-12)
12. 32CFR §2002(ee) - <https://www.govinfo.gov/content/pkg/CFR-2017-title32-vol6/pdf/CFR-2017-title32-vol6-part2002.pdf> [↑](#footnote-ref-13)
13. 32CFR §2002(rr) - <https://www.govinfo.gov/content/pkg/CFR-2017-title32-vol6/pdf/CFR-2017-title32-vol6-part2002.pdf> [↑](#footnote-ref-14)
14. 32CFR §2002(tt) - <https://www.govinfo.gov/content/pkg/CFR-2017-title32-vol6/pdf/CFR-2017-title32-vol6-part2002.pdf> [↑](#footnote-ref-15)