**DRAFT – Code of Professional Conduct and Adjudication Process**

# Executive Summary

## Code of Professional Conduct

This document establishes the Code of Professional Conduct for the CMMC Ecosystem. As such the document establishes standards and expectations that those in the ecosystem are expected to abide. This document is also the baseline by which concerns can be raised to the CMMC-AB about a participant in the ecosystem.

The Code of Professional Conduct includes the following key principles: 1) Professionalism, 2) Objectivity, 3) Confidentiality, 4) Proper use of Methods, and 5) Information Integrity. Undergirding those principles is also a respect for Intellectual Property and Implementation practices.

## Adjudication Process

This document also establishes the Adjudication Process by which the CMMC-AB will handle concerns raised by one party about another party in the ecosystem. Such concerns will need to be based in substance and linked to alleged deviations from the Code of Professional Conduct.

While the Adjudication Process is not solely for the case of an Organization Seeking Certification (OSC) to challenge the outcome of their assessment, this document does describe that process. The summary of that process is as follows:

Upon completion of a certified assessment, an Organization Seeking Certification (OSC) that does not achieve their planned CMMC Maturity Level, and believes the assessment result was due to errors, malfeasance, or ethical lapses by the Certified Assessor or C3PAO, is entitled to submit an adjudication request for consideration to the Accreditation Body (AB).

The OSC must submit their adjudication request, along with specific description and/or evidence of such lapses along with the list of the controls and/or practices in question, within 30 days after the completion of the Phase II (onsite) portion of their assessment.

Upon receipt of the adjudication request, a Certified Quality Auditor (CQA) from the AB staff will perform a preliminary evaluation of the Assessor or C3PAO's certification, training, and licensing, and will validate their adherence to the Code of Professional Conduct (CoPC) and the CMMC Assessment Methodology (CM2AM).  The OSC will be notified of the result of the preliminary evaluation, and given the opportunity to either accept the recommendation of the CQA, or to request secondary evaluation.

A secondary evaluation will be conducted if the OSC has a reasonable belief that the preliminary evaluation did not address the issues raised in the adjudication request.  During a secondary evaluation the CQA, who is also a Certified Assessor, will plan and conduct an onsite "delta assessment" of the controls and/or practices in question, and once completed, will submit the results, along with a recommendation, to the AB.  AB quality staff will evaluate the result of the secondary evaluation and inform the OSC of the final result of the adjudication process.

Adjudicated assessments that result in a successful CMMC Maturity Level certification for the OSC will retain the validity period of three years from the last day of Phase II (onsite) of the original assessment.

## 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.

**Agreement**

Agreement means any contract between two legal entities.

**Credentialed**

Credentialed refers to an individual who is applying to become, or is already ia Provisional Assessor, Certified Assessor, Certified Instructor, Certified Master Instructor, or Certified Quality Auditor

**Registered**

Registered refers to any person or organization that has taken appropriate training and is Registered on the CMMC-AB Registration Directory

**Accredited**

Accredited refers to any organization that is applying to become, or is already, a C3PAO, Licensed Partner Publisher, or Licensed Training Provider

**Partner Business Point of Contact**

Partner Business Point of Contact means any individual that has signature authority from a Licensed Partner to commit the Licensed Partner to the Code of Professional Conduct or an agreement with the CMMC Board.

**Solicit Business**

Solicit Business means to actively seek business or work from a customer, either by initiating the services, advertising the services, or encouraging a discussion about one’s services.

**Termination Without Cause**

Termination Without Cause means either party (CMMC License Partner, CMMC-Credentialed Individuals) may terminate their agreements at any time, with or without cause, with written notice to the other party thirty (30) calendar days prior to the date specified in such notice.

# Introduction

## Purpose

The Code of Professional Conduct (COPC) sets expectations for those CMMC-AB credentialed individuals and accredited organizations that are authorized to deliver CMMC services under license from the CMMC Accreditation Body (CMMC-AB). It also sets expectations for those Registered Practitioners and Registered Provider Organizations that deliver unlicensed non-certified services that choose to register with the CMMC-AB.

This CoPC represents the performance standards by which the roles of the CMMC eco-system will be held accountable, and the procedures for addressing violations of those performance standards.

This Code helps members in situations where we may be asked to compromise our values and integrity.

## Affected Persons and Organizations

The Code of Professional Conduct applies to:

* CMMC-AB Certified Professional
* CMMC-AB Certified Assessor
* CMMC-AB Certified Instructor
* CMMC-AB Certified Master Instructor
* CMMC-AB Certified Quality Auditor
* Certified Third Party Assessment Organization
* CMMC-AB Register Practitioner
* CMMC-AB Registered Provider Organization
* Licensed Partner Publisher
* Licensed Training Provider

# Guiding Principles

The Code of Professional Conduct is defined by the following guiding principles:

* Professionalism
* Objectivity
* Confidentiality
* Proper use of Methods
* Information Integrity

## Professionalism

Maintain a professional business posture at all times.

## Objectivity

The principle of objectivity imposes the obligation to be impartial, intellectually honest, and free of conflicts of interest. A CMMC professional should avoid the appearance of, or actual, conflicts of interest where possible, and fully comply with Conflict of Interest policies that may be signed as part of license agreements. In the case where a perceived or management conflict may be present, document and describe the conflict to all affected parties and secure agreement to continue.

## Confidentiality

As a credentialed, registered, or accredited professional or organization, you must maintain the confidentiality of customer and government data. You may be made aware of certain confidential information that is acquired in the performance of professional services, including data, trade secrets, business strategies, security postures, and personal information that may be contained within the systems you are exposed to. Treat confidential information with the utmost care, and under no circumstances reveal information learned during the delivery of CMMC services to anyone who is not expressly authorized to view it.

## Proper Use of Methods

Demonstrate integrity in the use of materials and methods as they are described by the CMMC AB in policies, methodologies, and training materials, and act in a manner consistent with the intent of the materials to preserve the integrity of CMMC service delivery.

## Information Integrity

Report results from the delivery of CMMC services completely and with integrity as required by your license or certification agreement.

# Practices

## Professionalism

1. Maintain an honest disposition with colleagues that results in a respectful exchange at all times.
2. Fulfill all commitments as defined by the contract, methods, or license, certification, or registration agreements.
3. Do not mislead or exaggerate the services that you are accredited or registered organization is authorized to deliver.
4. Do not mislead or exaggerate the services that you, as a credentialed or registered individual, are authorized to deliver.
5. As an accredited organization, ensure that only CMMC-AB Credentialed individuals are delivering CMMC assessment or training services.
6. Deliver CMMC services according to the agreements with your customer and the CMMC Accreditation Body.
7. Do misrepresent your organization, such as selling services for which you are not accredited to deliver, falsifying records or experience, or proposing fees that are far below the level of effort that is required.
8. Avoid all real and perceived Conflicts of Interest to the extent possible. When conflicts are unavoidable, disclose them transparently to affected stakeholders, including your own organization and your customer. Take action to minimize the impact or eliminate the conflict.
9. Under no circumstances are credentialed or registered individuals permitted to conduct a certified assessment, or participate on a certified assessment team, if they have also served as a consultant to prepare the organization for that assessment. Consulting is defined as “providing direct assistance to the creation of processes, training, and technology required to meet the intent of CMMC controls and processes.”
10. For C3PAOs, ensure that when your sponsored CMMC-Credentialed individuals are performing services for another party, they do not actively solicit business from the customer for themselves or your organization. When approached by a customer while performing services for another party, CMMC-Credentialed Individuals are to defer the discussion to a time outside the scope of the immediate work.
11. Do not make guarantees of assessment results. This includes guarantees that an Organization will succeed in their assessment if they engage with a credentialed individual or accredited organization, or the offer of a “money back” guarantee.

## Confidentiality

1. Protect customer data unless you have explicit permission to disclose it.
2. Proactively dispose of information that can be described as privileged information that is gathered during assessments or consulting. Exercise due care to ensure that confidential or privileged information remains so, even after a work engagement has ended.
3. Do not copy materials or tools from external organizations without explicit permission to do so.

## Adherence to Materials and Methods

1. Maintain current knowledge of CMMC materials. Relevant materials include, but are not limited to:
   1. C3PAO Guide
   2. C3PAO License Agreement
   3. LPP License Agreement
   4. LTP License Agreement
   5. Code of Professional Conduct
   6. Conflict of Interest Declaration
   7. Register Professional Agreement
   8. Registered Organization Agreement
   9. The CMMC Model
   10. The CMMC Assessment Guide
   11. The CMMC Assessment Methodology CAM)
2. Maintain compliance with CMMC-AB materials and methods.
3. Do not create derivative works using CMMC-AB or DOD Intellectual Property without explicit written permission by from the CMMC Accreditation Body.
4. For Assessors or assessment team members, participate actively and respect the boundaries of the role you are performing. Do not use the influence of a role in a manner that is inconsistent with the Assessment method or guide,
5. Do not make assertions about outcomes or assessments, training classes, exams, or other results before or during any CMMC event you are participating in.
6. Do not unfairly influence outcomes in any way, including coaching people to provide false or misleading information, providing answers or hints to exam questions, creating documentation that is not actually used, or offering competing services.

## Information Integrity

1. Report results and data from and Assessments Training objectively, completely, clearly, and accurately.
2. Ensure the accuracy and authenticity of information
3. Ensure the security of all information discovered or received during the course of delivering CMMC services
4. Do not allow cheating on examinations
5. Do not fill out evaluation materials for others.

## Respect for Intellectual Property

1. Ensure that you have the right to use or view any intellectual property during the delivery of CMMC services
2. Respect copyrights, trademarks and logos. Give appropriate references and credit to CMMC-Credentialed materials and sources.
3. Do not use CMMC-AB logos, trademarks, or copy written material with explicit and written permission from the CMMC-AB
4. Unless such permission is included in your agreement, always obtain written permission for distributing or changing materials, and for including materials in other works.

# Adjudication Process

Actions that are in violation of this Code must be investigated and adjudicated

## Oversight and Governance of Investigations and Adjudication Processes

The CMMC-AB shall establish and maintain an “Investigation and Adjudication” committee to the Board. This committee will be chaired by a duly elected board member and shall be staffed in accordance with the charter and election protocols established therein.

The CMMC-AB Investigation and Adjudication committee shall have the obligation to oversee, guide and direct any and all investigations and adjudication activities within the CMMC ecosystem unless otherwise established or directed by the CMMC-AB. The committee will make recommendations for which matters should not be investigated to the CMMC-AB for approval. Such instances where a matter will not be investigated could include but are not limited to duplication of prior investigation and/or insufficient details in the matter to afford an investigation. All other matters submitted will be investigated.

The CMMC-AB Investigation and Adjudication committee shall make regular reports and updated to the CMMC-AB regarding the status and results of their activities including all investigations and adjudication outcomes.

## Reporting of Matters for Investigation by non CMMC-AB board or Staff

When observing colleagues making choices that are in violation of the CoPC, as a CMMC professional you should privately request clarification or offer help rectify the violation. However, if clarification or help is not effective to resolve the issue, or if you believe corrective action is required to resolve the situation, then it is expected that you will submit a matter for investigation.

The CMMC-AB and by extension their Investigation and Adjudication committee will make available a mechanism for reporting matters for investigation. This mechanism will afford a member of the CMMC ecosystem the ability to report any matter for investigation. This might but is not limited to include both ethical and methodology concerns. The reporting mechanism will allow for both named and unanimous reporting of matters for investigation.

The CMMC-AB and by extension their Investigation and Adjudication committee will publish and otherwise make known the mechanisms (e.g. websites, hotlines or mailing addresses) by which matters for investigation will be collected.

## Reporting of Matters for Investigation by CMMC-AB board

The CMMC-AB monitors the CMMC-related activity of all CMMC credentialed, Registered, and Accredited roles and reserves the right to report matters for investigation related to any potential violations that arise from unusual behavior. CMMC Certified Quality Auditors, CMMC-AB staff and/or board members will initiate a Matter for Investigation via the same mechanisms noted above.

## Investigation Process

The CMMC-AB and by extension their Investigation and Adjudication committee will receive all Matters for Investigation that are reported. The committee will review and assign investigators that are not party to the matter at hand. For items where an investigation is not feasible or required, the committee will vote by simple majority to recommend to the CMMC-AB that the Matter for Investigation not be the subject of an investigation. If the CMMC-AB concurs the Matter for Investigation will be closed at that point. If the CMMC-AB disagrees the committee will assign an investigator and proceed and/or execute other instructions as provided by the CMMC-AB.

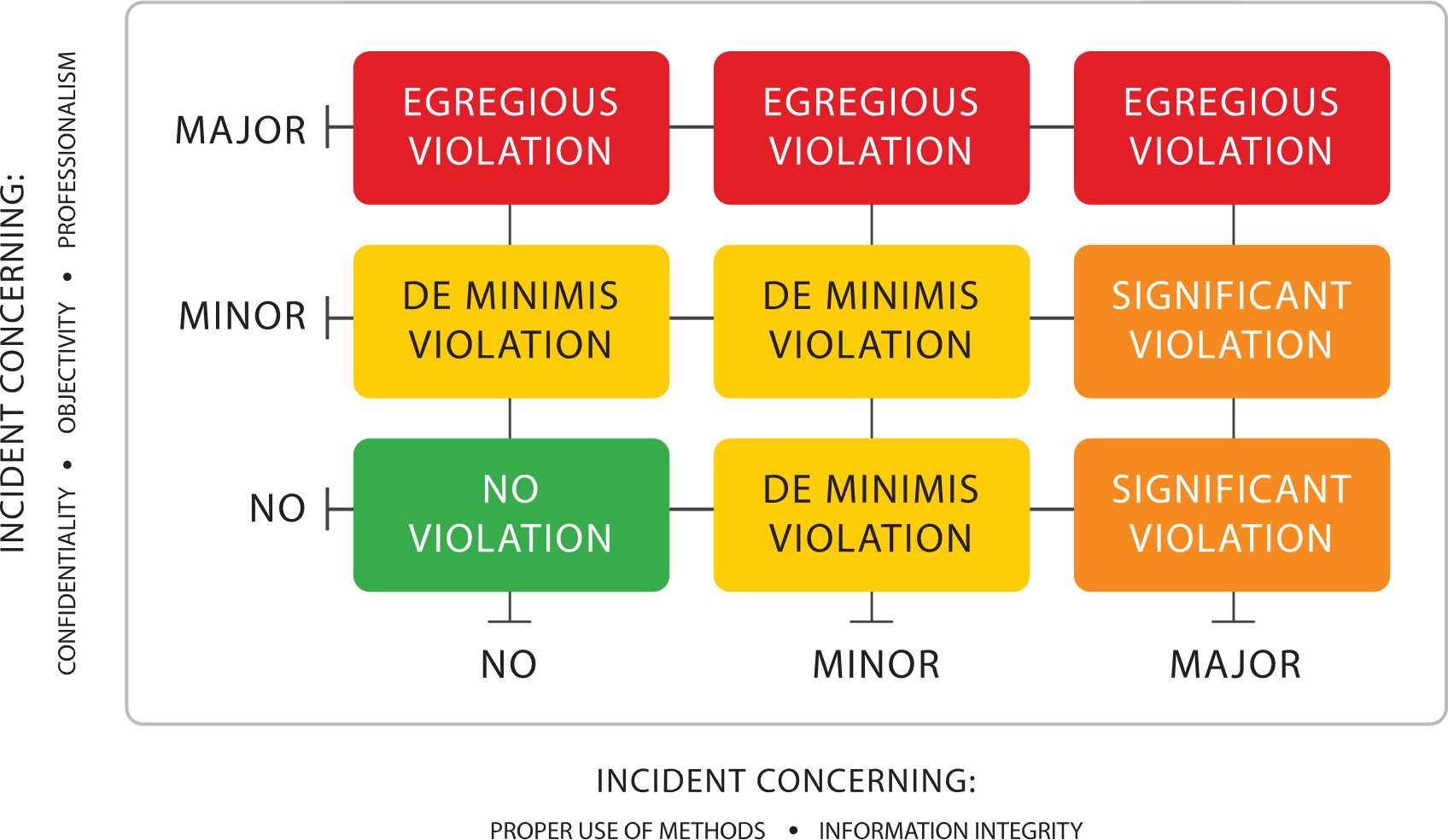
The Investigation and Adjudication committee will be responsible for identifying and training those individuals who will complete the investigations. Those investigators will similarly be expected to adhere to this Code of Professional Conduct to the extent applicable. Further, the investigators will confirm to the committee that they are not party to the Matter for Investigation (i.e. subject of or submitter of the matter), affiliated with, and/or subject to undue influence from such parties.

During the investigation, every effort will be taken to protect and respect the rights and the privacy of those involved. The subject of the investigation will be notified that they are being investigated. The CMMC-AB or by extension the Investigation and Adjudication committee will make determination and establish standards related to the release and timing thereof the Matter for Investigation submission and final reporting.

The appointed investigator will take those steps they determined needed to fully understand the situation. At the conclusion of their procedures, the investigator will prepare a report, either oral or written, for presentation to the CMMC-AB Investigation and Adjudication committee.

## Review of Investigative Proceedings and Adjudication

The Investigation and Adjudication committee will be responsible for receiving the Investigators report. Based on a review the committee will then instruct the investigator of additional procedures or make a recommendation to proceed to adjudication. If the committee, proceeds to adjudication that committee will utilize the following rubric as a guideline for such deliberations:



Major violations will be defined as:  
A deviation that represents a serious departure from this Code of Professional Conduct that could call into question the integrity of the CMMC or the reputation of those participating in or subject to the complaint.

Minor violations will be defined as:

A deviation that represents a less significant departure from this Code of Professional Conduct that is less likely to call into question the integrity of the CMMC or the reputation of those participating in or subject to the complaint

The rubric then establishes the following categories of violations which are defined as follows:

Egregious Violation – This category represents a major deviation from the Professionalism, Objectivity, and/or Confidentiality principles that are likely to call into question the integrity of CMMC or the ecosystem. If this incident(s) was also related to a violation of the Proper Use of Methodology or Integrity of Information principles it would tend to be intentional behavior that was not accidental or inadvertent.

Significant Violation – This category represents a non-major deviation from the Professionalism, Objectivity, and/or Confidentiality principles. However, there could be a major violation in the principles of Proper Use of Methodology and Integrity of Information. This a major Proper Use of Methodology and Integrity of Information violation it would tend to be an accidental or inadvertent violation.

De Minimis Violation – This category represents a minor violation from any of the principles and the CMMC-AB is confident this would not impact CMMC outcomes (e.g. assessments or accreditation efforts).

No Violation – This category does not represent a violation of any of the principles. Accordingly, this does not warrant disciplinary action. However, there are cases where this could be a learning point for the individual and such feedback would be communicated.

Ultimately it is at the discretion of the CMMC-AB and by extension the Investigation and Adjudication committee to make recommendations related to the violation categories assigned to an incident(s).

The Investigation and Adjudication committee will summarize the facts of the incident(s), provide a scoring according to the rubric and provide a recommend violation category as well as suggested disciplinary results. This will constitute a recommendation to the CMMC-AB. The board will be presented this package and will have the ability to deliberate, accept, reject or otherwise instruct the committee to engage in further actions until a resolution is reached that is satisfactory to the CMMC-AB.

## Corrective and Disciplinary Actions

The violation category recommended an ultimately accepted by the CMMC-AB will have corresponding corrective and disciplinary actions. Corrective actions may include warning, remediation, suspension, or termination of CMMC Credentials, Registration, or Accreditation. The Investigation and Adjudication committee will make recommendations to the CMMC-AB. The CMMC-AB has sole authority to determine the action to be taken.

Based on the violation category the following are the suggested levels of disciplinary action that can be modified at the sole discretion of the CMMC-AB.

Egregious Violation – Suspension or expulsion of the credentialed, certified or accredited party / parties. If the incident(s) adversely impacted or are likely to have adversely impact assessments, then the CMMC-AB will develop a plan to inspect the ALL of the last 6 months’ worth of assessments and further consequences could result.

Significant Violation – Probationary period or suspension of the credentialed, certified or accredited party / parties. If the incident(s) have a remote likelihood to have adversely impacted but not impossibility to adversely impact assessments, then the CMMC-AB will develop a plan to inspect a sample of the last 6 months’ worth of assessments and further consequences could result.

De Minimis Violation – A warning will be issued to the party’s / parties’ record(s). Repeat warnings / occurrences can result in an escalation.

In the event of termination of credential or license agreement, the termination will be conducted in accordance with the provisions of that agreement or credential in writing, thirty (30) calendar days prior to the date specified in such notice.

## Corrective Action Appeal

If a party has been subject to a corrective action and wish appeal the outcome with the CMMC-AB, you may request a review within 30 days of adjudication notice.

# Signifying your Agreements to the Terms of the Code of Professional Conduct

Committing to this Code of Professional Conduct is during the application process for your credentialed, registered, or accredited role.

# 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)