

Security Review of Article Submissions

Authors in government service, writing on subjects related to their areas of government expertise or work and whose article may derive from government information, are responsible for ensuring that articles receive the proper security review from the appropriate government authorities at their places of work. These reviews should be done before submission to the Military Intelligence Professional Bulletin. If required, these reviews should include vetting by both the organization's security officer and public affairs officer.

Articles by U.S. military personnel on active duty or civilian employees of the Department of Defense or service departments are subject to the official clearance requirements of Army Regulation 380-5. This requirement applies to documents that discuss the activities or capabilities of specific military organizations, established tactics, techniques, and procedures, or technical subjects, open discussion of which has the potential to expose information that is classified, sensitive, or should be regarded as otherwise controlled.

Current Army policy stipulates articles discussing these subjects of a technical nature or a current organization, which are written by personnel working for the U.S. Government as an employee or contractor, must include a memorandum for record verifying security review by the writer's organization of assignment. This memorandum should contain the words "This article does not include classified, sensitive, or controlled unclassified information and has no distribution restrictions" and be signed physically or electronically by the reviewing security authorities. It may be sent electronically as an Adobe PDF or Word document with appropriate signatures and accompanying electronic versions of the articles. An example memorandum is included.

Documents submitted by non-U.S. Government employees or contractors or by non-American authors who are not associated with or employed by the U.S. Government do not usually require a memorandum for record verifying a security review. Authors who are not employees of the U.S. government typically do not need a security review unless the source material appears to be from a source inside the government that could represent an unauthorized breach of confidentiality or seems to be proprietary information of a private organization. It is incumbent on authors of these articles to resolve any legal issues associated with their articles before publication.

Since MIPB is a public facing journal; any submission containing Controlled Unclassified Information (CUI) will be prepared for publishing to our sister journal MI Digest and must include appropriate Identification, Marking, and Dissemination information. Authors submitting content to the MI Digest are responsible for ensuring their articles receive the proper security review from their respective organizations prior to submission.

Unit Address

Office Symbol

Date

MEMORANDUM FOR RECORD

SUBJECT: INFOSEC and OPSEC Release for **Article** by **Author**

1. References:

- a. AR 380-5, Army Information Security Program, 22 October 2019.
- b. AR 530-1, Operations Security, 26 September 2014.

2. Enclosure: **Title and Author**.

3. The undersigned verifies that the enclosed article and accompanying graphics do not include classified, sensitive, or controlled unclassified information and have no distribution restrictions in accordance with references 1a and 1b.

4. Prior to publication and release to the public, the undersigned understands the Military Intelligence Professional Bulletin staff will obtain additional review from the USAICoE public affairs office and when necessary legal services for the enclosure.

5. POC for this memorandum is the undersigned at **COMM**, **DSN**, and **e-mail address**.

Signature Block

CUI Identification, Marking, and Dissemination

CUI is sensitive information that does not meet the criteria for classification but must still be protected. It is Government-created or owned UNCLASSIFIED information that allows for, or requires, safeguarding and dissemination controls in accordance with laws, regulations, or Government-wide policies.

CUI Identification

TO START, go to the DoD CUI Registry at <https://www.dodcui.mil>



Select the organizational index that best fits the type of information in your document. *For example, is it export control information or law enforcement information.*

Review the categories under the organizational index. Select the category your information is likely to fall under.

Review the information and authorities to determine the correct category. *The information must fall under a law, regulation, or government-wide policy for it to be identified as CUI.*

**CLEARED
For Open Publication**

10
Aug 29, 2025

Department of Defense
OFFICE OF PREPUBLICATION AND SECURITY REVIEW

CUI Marking

Markings are for training purposes only.

Required markings:

- “CUI” at the top and bottom of the page
- CUI designation Indicator block

Portion marking is optional but recommended.

The CUI designation indicator block will tell holders of the document:

- The organization the document came from
- The CUI categories identified in the document
- The authorized recipients of the document
- POC information

CUI

Controlled by: OUSD(I&S)/IAP
CUI category: BUDG
LDC: FEDCON
POC: osd.pentagon.rsrcmgmt.list.
osd-intel-infosec-mbx@mail.mil

CUI

CUI Dissemination

The 3rd line of the CUI designation indicator block tells you who the authorized recipients are. This line will normally indicate the limited dissemination control (LDC) but could also contain a distribution statement (required for CTI and EXPT).

The absence of an LDC or distribution statement means anyone with a lawful government purpose is permitted access to the information, but it does not imply public release.