GUIDE TO CONTROLLED UNCLASSIFIED INFORMATION (CUI) MARKINGS

CUI Marking Requirements and Management in Microsoft Applications

archTIS

TABLE OF CONTENTS

EXECUTIVE SUMMARY

In July 2022, the Pentagon's acquisition office issued a memo reminding acquisition officials of the DoD's requirements for handling controlled unclassified information (CUI).

The standard which applies to Defense contractors is not new. The original Defense Federal Acquisition Regulation Supplement (DFARS) clause 252.204-7012 requirement went into effect in 2017. With a renewed focus on protecting CUI and several regulations governing its handling, including CMMC 2.0, understanding CUI protection is of utmost importance to all US Government agencies, Defense contractors and suppliers.

What is CUI?

Controlled Unclassified Information or CUI is defined as government-created or owned information that requires safeguarding or dissemination controls consistent with applicable laws, regulations and government-wide policies, including the soon-to-be-released CMMC 2.0, DFARS clause 252.204-7012, NIST Special Publication 800-171 and ITAR.

The security requirements are built on the principle that certain types of unclassified information are extremely sensitive, valuable to national security, sought after by strategic competitors and adversaries, and may also have legal safeguarding requirements. The CUI policy aims to standardize the CUI marking system across the Federal Government, replacing agency-specific markings such as FOUO, LES, SBU, etc.

What's at Stake?

Improper safeguarding or loss of controlled unclassified information could potentially have serious adverse effects on organizational operations, organizational assets, and/or individuals. Any of these scenarios could result in a degradation in mission capability, damage to organizational assets, financial loss or harm to individuals.

As with many other regulations, the new CMMC Level 2 requirements will follow the 110 security controls of NIST SP 800-171 developed to protect CUI. Defense contractors handling CUI have been required to comply with NIST SP 800-171 since 2017 as part of their DFARS contract obligations. If you're already in compliance with NIST SP 800-171, you've got a jump start.

CUI Classification Categories

CUI falls within one of 125 categories under the following groups:

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

DOD MARKING GUIDELINES

If you have CUI it needs to be marked accordingly. The purpose of CUI markings and the CUI Designation Indicator is to inform or alert recipients and/or users that CUI is present and of any limited dissemination controls.

Controlled unclassified information (CUI) falls within one of 125 categories under the groups in the call out on the left. Be sure to identify the category and the necessary markings and controls for the information that you are handling. A full list of CUI categories and the required banner markings and dissemination controls for each can be found here.

Here's a summary of the DoD's guidance on CUI Markings for Unclassified and Classified documents.

Unclassified Documents Containing CUI

- Place "CUI" at the top and bottom of each page.
- Portion markings are optional on unclassified documents, but if used, all portions will be marked.
- The CUI designation indicator will be placed at the bottom of the first page or cover of all documents containing CUI:
  - Line 1: The name of the DoD Component (not required if identified in the letterhead)
  - Line 2: Identification of the office creating the document
  - Line 3: Identification of the categories contained in the document
  - Line 4: Applicable distribution statement or limited dissemination control (LDC)
  - Line 5: Name and phone number or email of POC

Classified Documents Containing CUI

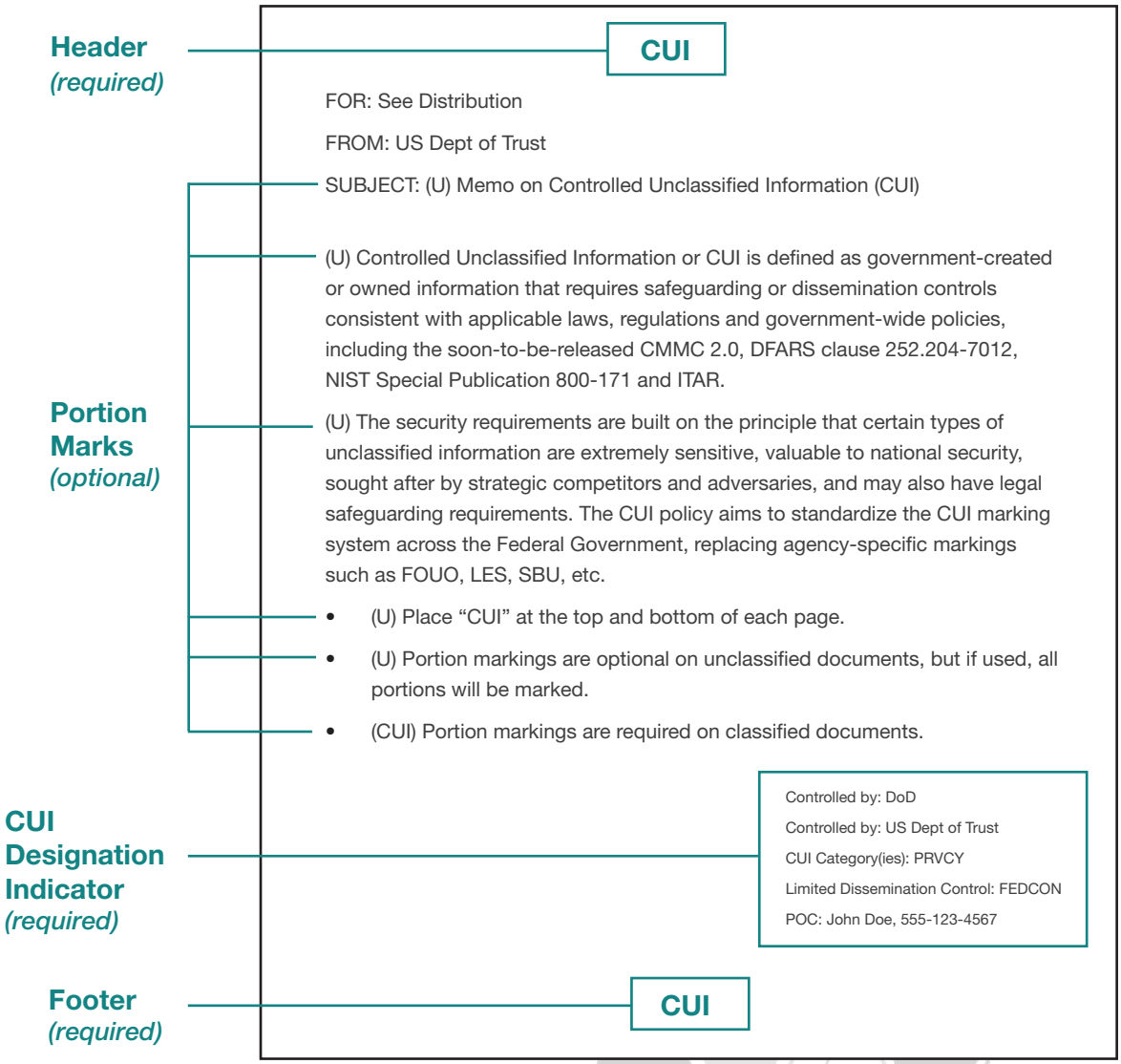
- "CUI" does not go into the banner line.
- The CUI designation indicator and the classification authority block will be placed at the bottom of the first page.
- Portion markings are required on classified documents.
- Classified documents will be marked IAW DoDM 5200.01 Volume 2.
- CUI markings will appear in portions known to contain only CUI.
- A warning statement will be placed at the bottom of the first page of multi-page documents alerting readers to the presence of CUI in a classified DoD document.

Portion Marking

Though not required for CUI, portion markings identify what specific information belongs to specific CUI Categories or has specific Limited Dissemination Controls within a document. Portion markings are placed at the beginning of the section to which they apply and must be used throughout the entire document. This includes subjects, titles, paragraphs and subparagraphs, bullet points and sub-bullet points, headings, pictures, graphs, charts, maps, reference lists, etc. Portions containing CUI are denoted (CUI). Portions that do not contain CUI can be denoted as Uncontrolled (U).

Refer to the Department of Defense CUI Marking Guide for detailed instructions on CUI labeling and portion marking.

REQUIRED CUI MARKINGS FOR UNCLASSIFIED DOCUMENTS



archTIS

Microsoft Partner

Member of Microsoft Intelligent Security Association

> *"Our Aerospace and Defense Industrial Base customers and partners are actively seeking a product that can help meet zero-trust requirements, especially in respect to demonstrating compliance with the new CMMC standards for the secure handling of Controlled Unclassified Information.*
>
> *The innovative content watermarking capability from NC Protect makes it painless to add the required CUI Designator Label to meet compliance.*
>
> *More importantly, NC Protect works in concert with Microsoft Purview Information Protection to secure and encrypt the content leveraging a data-centric, zero-trust methodology ensuring recommended practices for information security and data handling."*
>
> *Richard Wakeman*
> *Chief Architect, Aerospace & Commercial Defense, Microsoft*

WHY TAGGING AND MARKING CUI CAN BE A COMPLEX ENDEAVOR

Managing CUI in document management and collaboration systems like Microsoft 365 and SharePoint Sever can be complicated. First, data must be properly tagged/classified as CUI. Plus, a document's sensitivity level often changes over time. Sometimes unclassified information may become part of a classified program. Data needs to be tagged appropriately and monitored for changes in order to keep it safe from improper dissemination.

Relying on users to remember all of the classification and labeling requirements can be prone to error, which can lead to fines and or loss of contracts depending on the regulation. And while most regulations reference NIST 800-171, each has its own caveats. You want to ensure that you have tools in place that can help identify CUI, label it appropriately and restrict access according to the applicable regulation(s).

AUTOMATING CUI MARKINGS & DOCUMENT PROTECTION IN MICROSOFT APPLICATIONS

NC Protect provides a full range of capabilities to identify and protect CUI and other sensitive data, allowing users to automatically classify and apply a CUI Designator Label to documents.

Depending on the CUI level, user's geographic location and security privileges, NC Protect can apply dynamic protection to prevent visibility of the document to unauthorized users, prevent emailing, and/or display the document within NC Protect's secure ready-only viewer or allow the user to fully interact with the document.

With NC Protect dynamic policies, easily manage the tagging, labeling and security of CUI across Microsoft 365 applications (Teams, SharePoint Online, Exchange, Office and OneDrive), GCC and GCC High, as well as SharePoint on-premises.

Scan and Tag CUI

NC Protect also helps organizations protect CUI from improper access and/or release. It scans your document repository (SharePoint Online or Server, Teams, OneDrive, File Shares) and identifies files containing CUI. It then classifies the files according to its CUI level and restricts who in the organization can access the documents based on the document's classification and attributes such as security clearance and country.

Because NC Protect's access and protection policies are built using attributes, it can also leverage Microsoft Purview Information Protection (MPIP) sensitivity labels or classifications from other products (e.g., Janusseal, Titus, etc.) and use those values to apply markings and dynamic protection policies. Use NC Protect's classifications or a combination of these other classifications to suit your organization's taxonomy requirements.

Automatically Apply CUI Markings

NC Protect dynamically embeds CUI Designation Indicator markings including Owner Name, Controlled By, Category, Distribution/ Limited Dissemination Control and POC, as well as headers/footers into documents as a persistent watermark. When any protected document is opened in Microsoft Office or the NC Protect Secure Reader, the CUI Designation Indicator label is embedded in the file as a persistent watermark.

Dynamic Attribute-based Access Control (ABAC) and Data Protection Policies

NC Protect also provides robust access controls and data protection capabilities to safeguard CUI. Using ABAC, it evaluates both data, environment and user attributes against defined policies to determine appropriate access, usage and sharing rights for each and every document. It can control what a user sees when viewing and searching for files in Microsoft apps and determine if a user can open, edit, copy or download a file. It can also redact sensitive/classified information, such as keywords or phrases, in Word, Excel, PowerPoint and PDF, or when the file is presented in the Secure Reader.

Audit CUI Access and Activity

NC Protect audits user activity and permissions. It logs and tracks sensitive access, user actions such as producing, editing or deleting data, and general access. Easily ingest user activity logs collected in NC Protect into Microsoft Sentinel or Splunk to analyze the data at scale as well as trigger holistic alerts and remediation actions.

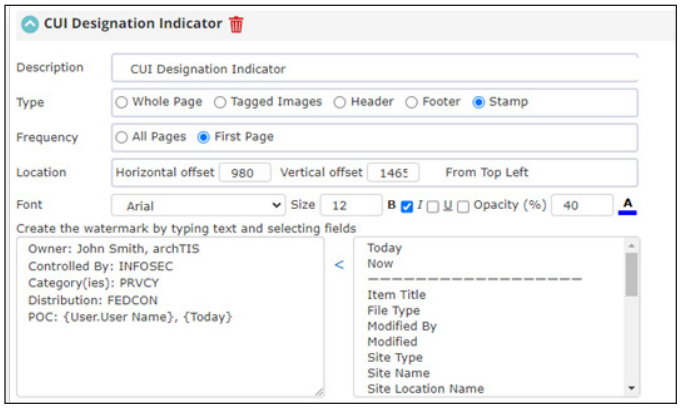
BUILDING CUI MARKING POLICIES WITH NC PROTECT

With NC Protect dynamic policies, easily manage the tagging, labeling and security of CUI across Microsoft 365 applications (Teams, SharePoint Online, Exchange, Office and OneDrive), GCC and GCC High, as well as SharePoint on-premises.

With NC Protect, CUI markings can be dynamically applied to documents as a persistent watermark when the file is opened and while at rest in your document library.

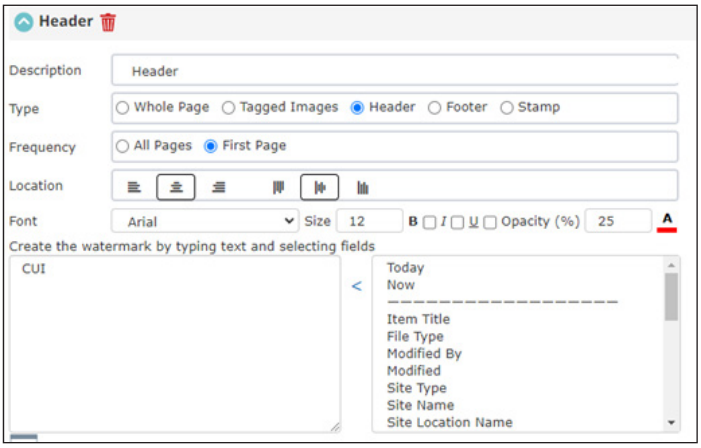
To apply CUI Markings to a document when it is opened or at rest, the user creates a Secure Document rule in NC Protect that controls how a document is viewed. A Secure Document rule uses data and user attributes to define when a CUI Marking should be added to a document.

For example, a document has been classified as containing CUI and the user's security clearance permits access according to the defined policy. When the users opens the document in the native application (e.g. Word, Excel), the appropriate CUI Markings will be dynamically applied by NC Protect as a persistent watermark.



Left: NC Protect's Secure Document rule builder contains a section for configuring watermarks, where the user will configure the Header/Footer and CUI Designation Indicator Labels. Additional details can be customized including: frequency (determines whether the watermark goes only on the first or every page), watermark location and color, and font style (font type, size, style, opacity).

Right: Header and Footer watermarks can be added using the same Secure Document rule. The header and footer configuration is the same as above, except for a different watermark type, and the Location now defines the alignment and orientation of the label.

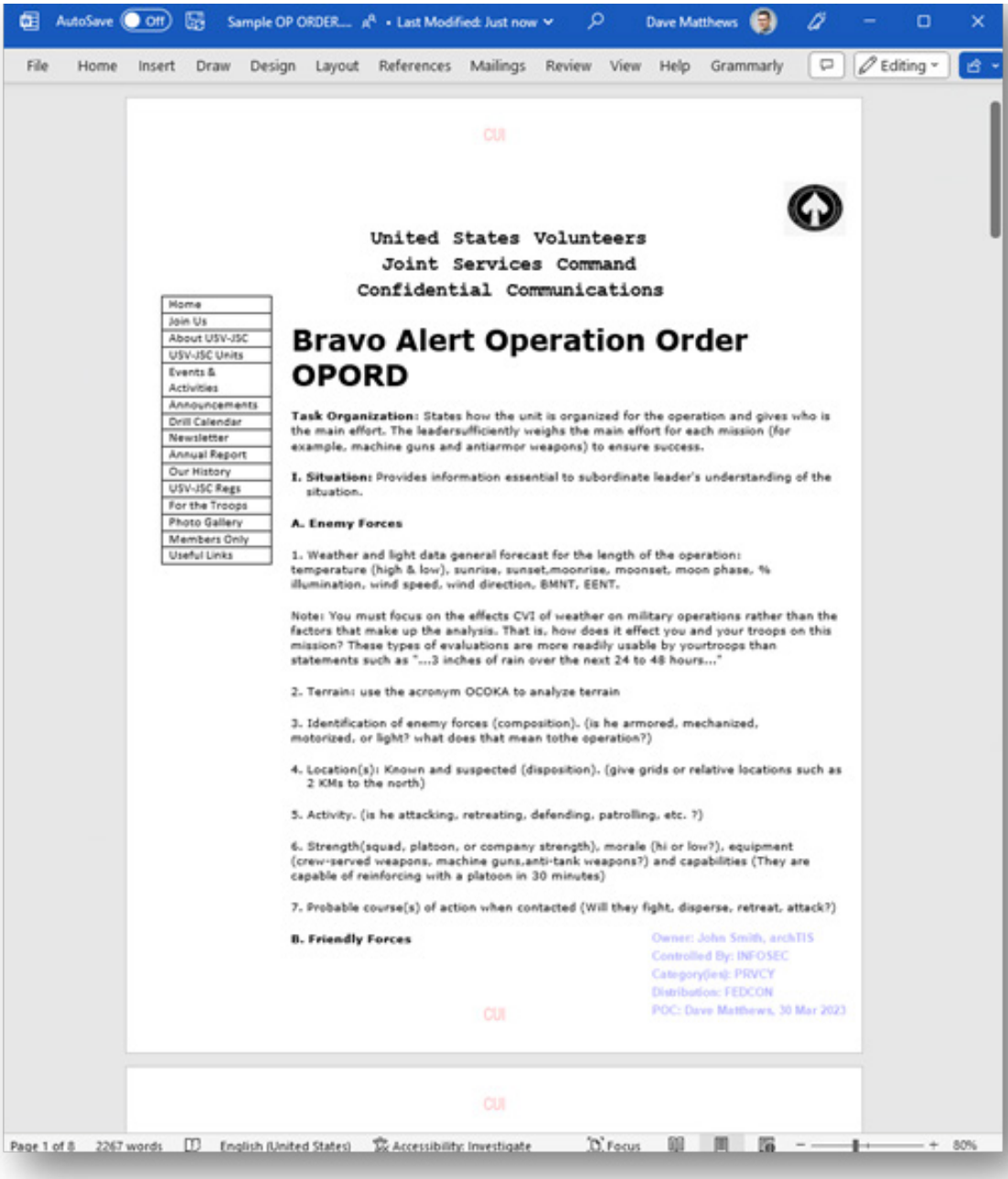


EXAMPLES OF CUI MARKINGS APPLIED AT REST AND IN USE

Marking Microsoft Office and PDF Documents

NC Protect can dynamically apply a CUI Designation Indicator Label and other visual markings such as headers and footers to data at rest using a persistent digital watermark.

It can also dynamically apply these same visual markings when the file is in use in Word, Excel, PowerPoint and PDF.

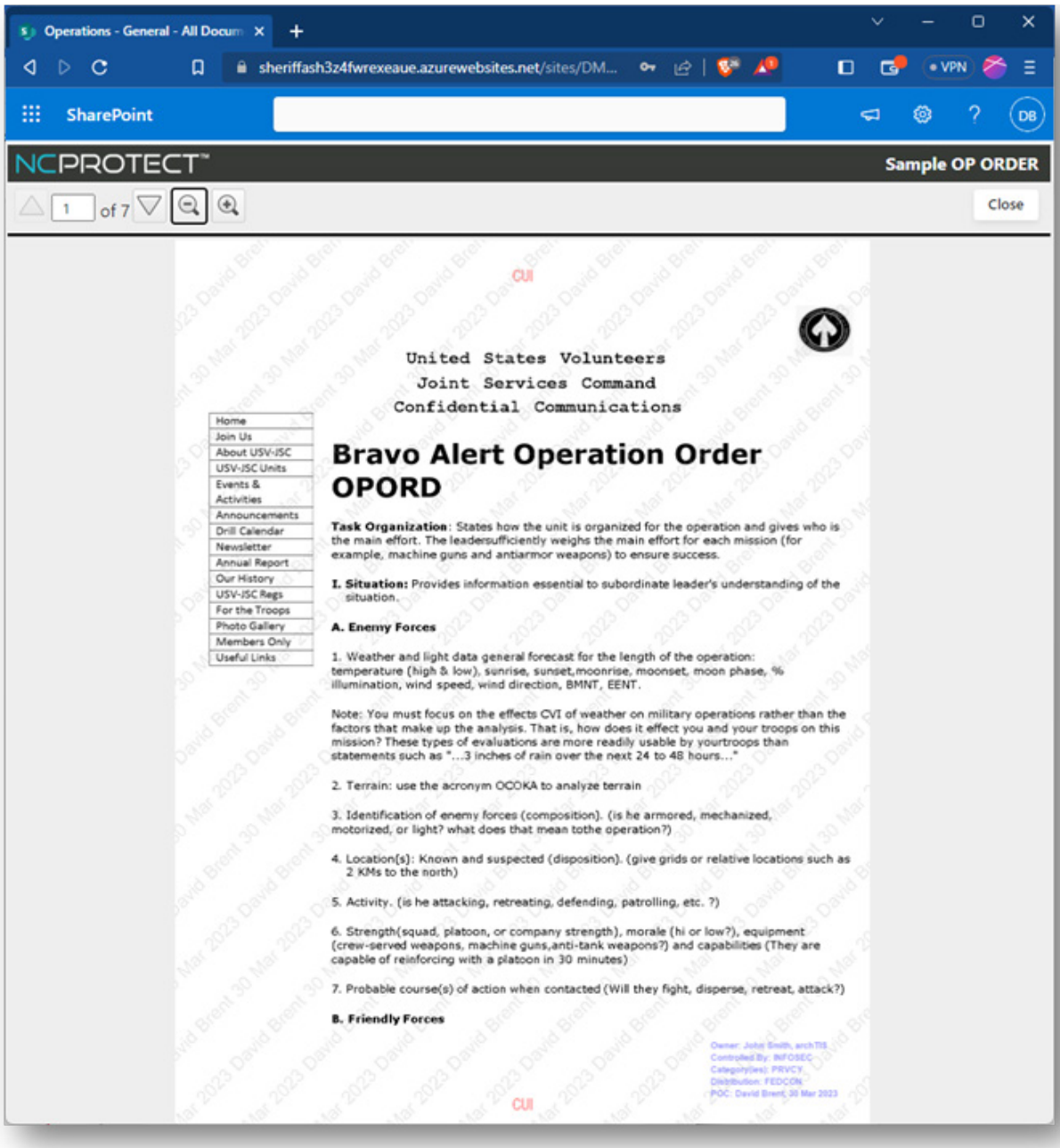


EXAMPLES OF CUI MARKINGS APPLIED AT REST AND IN USE

NC Protect Built in Secure Reader

Use the built-in NC Protect Secure Reader to present authorized users with a secure read-only view of the document. The Secure Reader prevents users from being able to save, copy, download or print the file.

For additional security, a security watermark can also be dynamically applied the document. These can include any predefined combination of attributes such as user name, date, time and location at the time of access. This additional security trimming deters users from snapping photos of sensitive information and assists in forensics in the event of a leak.



LET'S GET THE CONVERSATION STARTED

Don't wait for CMMC 2.0. Now is the time to get ready for the new CUI markings requirements.

NC Protect provides a full range of capabilities to identify and protect CUI and other sensitive data across Microsoft 365 applications (Teams, SharePoint Online, Exchange, Office and OneDrive), GCC and GCC High, as well as SharePoint on-premises.

NC Protect's flexible ABAC-based access and protection policies can easily be extended to other government regulations and requirements, including NIST, DFARS, ITAR and EAR, for a seamless solution to manage and automate information security and compliance.

Discover why NC Protect has been recognized by the Microsoft Security Excellence Awards as a Compliance & Privacy Trailblazer Finalist.

CONTACT US

www.archtis.com/contact

ABOUT ARCHTIS LIMITED

archTIS Limited (ASX:AR9) is a provider of innovative software solutions for the secure collaboration of sensitive information. The company's award-winning data-centric information security solutions protect the world's most sensitive content in government, defence, supply chain, enterprises and regulated industries through attribute based access and control (ABAC) policies. archTIS products include Kojensi, a multi-government certified platform for the secure access, sharing and collaboration of sensitive and classified information; and NC Protect for enhanced information protection for file access and sharing, messaging and emailing of sensitive and classified content across Microsoft 365, SharePoint Server, Nutanix Files and Windows file shares.

For more information visit archtis.com. Follow us on twitter @arch_tis.

archTIS

archtis.com | info@archtis.com

Australia | United States | United Kingdom