All Partners Access Network

CUI Standard Operating Procedures for Community Owners

April 22, 2025

Document Version

All published versions of this document are approved by the APAN Capability Lead and/or the APAN Technical.

Version	Editor	Date	Comments
1.0	Todd Hall	01/25/2019	Reviewed by Technical Director
1.1	Arlana DeLeo	02/22/2019	Minor edits for phone#, vendor app names
2.0	Arlana DeLeo	01/14/2021	Added links to official CUI policies/references, modified document organization and layout for consistency with other APAN SOPs; clarified roles, responsibilities, and procedures
2.01	Arlana DeLeo	03/10/2021	Clarified Adobe Connect access permission levels
2.02	Arlana DeLeo	06/23/2021	Changed verbiage from “stored” to “shared” to clarify any CUI being shared or discussed using APAN platform applications
2.03	Lucy Pabon	03/21/2023	Updated information on CUI published on non-CUI approved communities
3.0	Lucy Pabon	03/06/2025	Complete update of all content
3.1	Lucy Pabon	04/22/2025	Updated CUI training link

Contents

1. Background

This document provides All Partners Access Network (APAN) users and community owners with guidelines and procedures for requesting approval to share Controlled Unclassified Information (CUI) within an APAN community. Guidance contained in this document will be reviewed and updated on a yearly basis or at any time a new capability or feature becomes available on the platform.

A. APAN Operational Environment and Security:

1. **Security Controls**: APAN is maintained under an approved Authorization to Operate (ATO) (NOV 2023) from the United States Air Force, Headquarters Air Force, office of the Administrative Assistant to the Secretary of the Air Force (USAF HAF SAF/AA) and has been hosted within Amazon Web Services Government Cloud (AWS GovCloud) since August 2018. The assessment of security controls and other DoD requirements are based on the use of Department of Air Force Risk Management Framework utilizing NIST-800-53 rev 4. Data at rest and data in transit are always encrypted.
2. **Constraints for CUI storage**: All CUI requests must be approved in writing by the APAN Capability Lead and the APAN Technical Director. Storing CUI on the platform should always be for **a specific operation or event with a defined start/end date**. APAN is not a records management platform and is not intended for long-term storage.
3. **Responsible Parties**: The SAF/AA Mission Partner Capability Office (MPCO) has designated the APAN Application Service Provider as being responsible for maintaining the entire Operational Environment, to include CUI communities. Approval for hosting CUI within an APAN community is granted by the APAN Technical Director (or designee).

For technical questions regarding the APAN environment's status and security measures, users should submit a support ticket. As a DoD Enterprise Information Sharing Service, APAN's system information (e.g., security tool versions, ATO documents, Cloud Access Point (CAP) waivers, Risk Management Framework (RMF) Assessment and Authorization (A&A) documentation) is restricted and may only be shared with authorized DoD personnel outside the MPCO APAN Team with approval from the APAN Capability Lead or Technical Director.

B. Terms

1. **Community**: The term “community” refers to any site, group, portal, meeting room, or any type of collaborative workspace defined by any of the various applications.
2. **Content**: Any documents, dynamic web pages, imagery, audio recordings, data feeds, GIS/maps, virtual meeting room shared displays, chat transcripts, lists, galleries, libraries, wikis, blogs, discussion forums/boards, databases, calendars, or any other types of files/info shared on the platform.
3. **CUI**: Communities requiring Controlled Unclassified Information (CUI) protection have used the "CUI" label since March 2020. Previously, the label was "For Official Use Only" (FOUO). In this document, "CUI" refers to both current CUI and legacy FOUO within APAN.
4. **Primary Community Owner (PCO)**: previously the Portal Information Manager (PIM), is responsible for managing membership, content, and access attributes associated with the communities to which they are assigned as an owner or host. They are required to complete the pre-requisites for community ownership identified in section 3.Aof this document.
5. **Information Official (IO)**: The PCOs own command/organization Chief Information Officer (CIO), Foreign Disclosure Officer (FDO), Information Assurance Manager (IAM), Public Affairs Officer (PAO), or

Information Security System Manager/Officer (ISSM/ISSO) typically fills the role of IO; any Flag/General Officer (FOGO), Senior Executive Service (SES) Civilian or Staff Director is authorized to appoint an individual to act as the IO. The IO must be a government or military staff member, not a contractor.

a. The IO and PCO may not be the same person; the IO must be familiar with and comply with all DoD Information Assurance guidelines and abide by DoD policy for handling CUI.
b. The originator of information/documents is responsible for determining whether it may qualify for CUI status and applying the appropriate security markings; however, the IO should review and/or be aware of all the CUI content that is contained within a community.

C. APAN Community Owner Guidelines and APAN Applications Governance

1. APAN Community Owner Guidelines:
   https://community.apan.org/support/m/info/139431
2. APAN Applications - Generalized Governance for End-Users:
   https://community.apan.org/support/m/info/262852

D. Considerations for determining if APAN is a suitable platform for hosting CUI

All requests for posting and sharing of CUI must be approved in writing by the APAN Capability Lead and the APAN Technical Director regardless of the requirements or reasoning behind choosing to share CUI on APAN.

1. CUI often needs to be shared with individuals lacking access to secure networks like NIPRNet (e.g., during coalition exercises or multinational events). In operational settings like Humanitarian Assistance/Disaster Relief (HA/DR) or Defense Support of Civil Authorities (DSCA) where NIPRNet may be unavailable, sharing CUI via commercial internet (e.g., Wi-Fi, mobile broadband) with authorized partners is prioritized over restricting access due to network limitations.
2. APAN is designed to prioritize information sharing over information protection. However, even during HA/DR, DSCA, crisis response, or emergencies requiring CUI protection, CUI may NOT be uploaded to APAN without explicit written approval.
3. Command leadership (e.g., appointed IO) is solely responsible for determining whether to request approval to share CUI on their respective community. APAN staff may only confirm existing policies and guidelines and will not make any suggestions, recommendations, or provide guidance about whether a particular command should use the APAN platform to share CUI. Any questions or requests for clarification about platform stipulations may be resolved by APAN government leadership.

E. Remediation of Unauthorized CUI/PII Postings

System administrators will conduct random security checks to identify unapproved CUI, legacy FOUO, PII, or other unauthorized content. When such content is identified, the APAN Knowledge Managers (KMs) will notify the community owners of any violations, in most cases allowing them 24 hours to remove the content. KMs will delete any remaining unauthorized content after 24 hours. Deleted content will not be restored.

1. For security reasons, APAN administrators may remove content labeled as “CUI” or “FOUO” within an unapproved (unclassified-only) community on the platform at any time. Such content will ***not*** be restored.
2. Community Owners will be notified and must acknowledge adherence to previously stated guidelines in section 1.E of this document. Repeated violations of policy (unauthorized community ownership and/or unauthorized use of the platform) will be documented and may result in privileges being revoked and/or the entire community (and associated content/membership) being permanently removed.

2. Responsibilities

A. PCO Responsibilities

1. PCOs are Community Owners responsible for management of and access to CUI posted within their community; responsibilities include, but are not limited to:
    a. Provide complete documentation with the initial request for CUI approval, including CAC/PIV signature
    b. Attend required Community Owner Training acquainting them with PCO responsibilities
    c. Monitor and manage all community membership/access requests and posted content
    d. Strictly enforce least privileged access model for all CUI, granting access to authorized users only as determined by the IO
    e. Validate the user identity, user account name, and “need to know” before granting access. Limit posted CUI content to mission relevant items, posted sparingly.
    f. Regularly review posted CUI and purge any CUI no longer relevant to the operational situation
    g. Remove unauthorized CUI within 24 hours if identified.
    h. If combined unclassified information are potentially classified, purge the most sensitive information and notify the IO
    i. Notify APAN staff regarding any new sub-sites/sub-groups created within an approved CUI community so that banners are properly activated
    j. Respond to requests for information from APAN staff and/or community members
    k. Provide CUI guidance to community members and anyone posting content

B. IO Responsibilities

1. Review and complete documentation for the CUI approval form, including CAC/PIV signature.
2. Periodically review information shared within the approved CUI community to ensure only authorized CUI is posted and to maintain situational awareness of the types of CUI being shared.
3. Respond to requests for information from APAN staff and/or the community’s PCO.

C. APAN Staff Responsibilities

1. KMs:
    a. Process requests: Review user documentation (purpose/description, correctly completed fields, CAC/PIV signatures), notify user of the APAN Capability Lead and APAN Technical Director’s (or designee’s) decision to approve/deny request, and update internal documentation.

b. Activate banners for parent/top-level groups/sites and all associated/subsequent requests for CUI banner activation within sub-groups/ sub-sites.
c. Promptly respond to and maintain communication with the users regarding any content or membership safeguard concerns requiring action, whether initiated by the user or APAN Cybersecurity analysts. Delete expired communities. Process renewal requests for communities that remain active and have indicated a need for renewal. Delete unapproved CUI, PII, or other content that was not removed within 24 hours of notification by system administrators.

2. APAN Capability Lead and APAN Technical Director (or designee): Review and sign for final approval (or respond to indicate denial/non-concur) for CUI community requests.
3. APAN staff members will **not** provide recommendations, suggestions, or guidance regarding the posting of specific CUI to a CUI community, other than confirming the information documented on the approved request form.

3. Procedures

This outlines the process for requesting and maintaining CUI storage approval.

A. CUI Request

1. Preparation and Training:
   a. Request Ticket: Submit a "Request Something" ticket at https://esms.mpe.af.mil/mpco, selecting the "CUI Storage Approval" option.
   b. CUI Training: Complete the DoD Mandatory Controlled Unclassified Information (CUI) Training from your organization or from https://securityawareness.usalearning.gov/cui/ and obtain a current CUI training certificate. CUI training certificate must not expire within 30 days of requesting a CUI community.
   c. CUI SOP and Markings: Review the CUI SOP and ensure your request adheres to its guidelines. Determine the specific CUI categories and markings you will upload to APAN from the CUI Category Marking List https://archives.gov/cui/registry/category-marking-list. Cross-reference these with the disallowed categories in Section 5.B.4.b of this CUI SOP. CUI Specified categories are not permitted.
2. Form Completion and Submission:
   a. Community Owner Acknowledgement (COA) Form: Download, complete, and digitally sign (using CAC, PIV, or DoD/GOV digital certificate) COA form https://community.apan.org/support/m/info/139434.
   b. Community CUI Request Form: Download, complete, and digitally sign (using CAC, PIV, or DoD/GOV digital certificate) the CUI Request Form https://community.apan.org/support/m/info/139432. Provide the Category Marking from column 4 for all applicable categories in the “Description” https://www.archives.gov/cui/registry/category-marking-list. The "End Date" should be no more than two years from the request date, with a renewal option. This form requires signatures from both the PCO and the IO.
   c. Submit Documents: Attach the CUI training certificate and the signed COA and CUI Request forms to the Request Ticket.
3. Review and Approval Process:

a. KM Review: The designated KM will review the submitted forms and documentation and may request additional information or minor changes.
b. Lead KM Review and Approval: The Lead KM will review and forward the request to the APAN Technical Director (or designee) and APAN Capability Lead for review and signature.

4. CUI Designation and Notification:
   a. CUI Enablement: Upon approval, the designated KM will enable the group for CUI storage. A banner will automatically appear at the top of the group indicating official CUI approval.
   b. CUI Community Designation: The community will be permanently designated as CUI. All sub-communities will also be designated as CUI. Non-CUI sub-communities are not permitted under an approved CUI community. Changes to group or site settings related to CUI are not permitted after approval. If non-CUI sharing is required, a separate community must be created.
5. Notification: The KM will notify the user via the support ticket and update internal documentation.

B. CUI Community Renewal and Deletion:

1. Renewal Process: Within 30 days of the "End Date," the community (including all sub-communities and content) will be permanently deleted unless the user requests a renewal. A new request form must be submitted for renewals.
2. Renewal Notification and Deletion: The PCO is responsible for monitoring the CUI approval expiration date. If the current Community Owners, PCO, or IO do not respond to renewal requests from the KM within 10 business days, the CUI community, subcommunity, and their contents will be permanently deleted. This action is not recoverable.
3. Inactive Community Deletion: KMs will delete CUI communities that have been inactive (no content posted) for more than two years, according to the Retention Policy located in the APAN Applications Generalized Governance for End Users.

4. Application-Specific Details

A. Microsoft SharePoint Sites

1. Search and Offline availability settings, and Anonymous Access will be turned off.
2. No generic, enterprise-wide directory access (e.g., “Anonymous”, “NT Authenticated”, “All authenticated users”, “All Windows users”), is allowed for any elements of the site (including unique list, library, or document-specific permissions). These options are only permitted to be used on Public sites. If these settings are found in any non-public site, they will be removed.
3. Application controls are in place to prevent users from setting Alerts on lists or libraries, to prevent any CUI or attachments from being emailed.
4. If site owners modify or circumvent permissions/controls, potentially allowing unauthorized access, KMs will take the following steps to protect platform information: The PCO, IO, and any other Community Owners will be notified to immediately rectify the situation and/or may be required to attend remedial training.
5. Repeated community violations will be reported to the APAN Capability Lead and Technical Director, potentially resulting in the user losing data storage/management privileges on APAN and requiring their command/organization to appoint a new PCO.

B. Verint Groups

1. Group privacy will be set to and remain at “Private Unlisted”
2. “Content-less” delivery of e-mail subscriptions will be enacted with a warning displayed before files download. Subscribers to blogs or forums will receive notifications prompting them to log in to APAN and return to the community to view the posted content, rather than receiving the content directly via email.
3. If group owners/managers modify or circumvent permissions/controls, potentially allowing unauthorized access, KMs will take the following steps to protect platform information: PCO, IO, and any other Community Owners will be notified immediately rectify the situation and/or may be required to attend remedial training.
4. Repeated community violations will be reported to the APAN Capability Lead and Technical Director, potentially resulting in the user losing data storage/management privileges and requiring their command/organization to appoint a new PCO.

C. Other APAN Capability Tools / Applications

1. For all other tools/applications (e.g., Adobe Connect, Arc GIS or Chat) marked on the approved CUI request form, the Community Owner or Host must inform users that CUI is authorized.
    a. Diligently review access permissions for all information exchange capabilities with their community, complete required training, and correct any access-related problems identified by APAN staff.
    b. **Never record Adobe Connect meetings where CUI is discussed. APAN staff will immediately delete any such recordings without notice.**
    c. **Disable the "Anyone who has the URL for the meeting can enter the room" option in the Adobe Connect room access settings to prevent unauthorized access. Enabling this option would allow anyone on the Internet access to the room and uploaded content without being vetted/approved. Permitted access settings (in order of preference) are:**
        i. Registered users (Host approval required, recommended setting).
        ii. Account Members (Allowed, but not recommended). Anyone with an APAN account can join without being vetted/approved.
        iii. Accepted guests (Allowed, but not recommended). Hosts cannot confirm the identity of unauthenticated “guests”.
2. Community owners may contact the APAN Help Desk to request details and instructions for creating an HTML header/banner as needed.
3. Contact the APAN Help Desk for guidance on exporting content from the platform to their local network or other information systems.
    a. APAN staff will not export data for users, except for specific SharePoint document libraries. SharePoint export requests must be submitted by Community Owners (or IOs) at least 10 business days before the required delivery date.
4. If/when a CUI community is deleted, all associated Adobe Connect rooms, ArcGIS portal and/or Chat room content is also permanently deleted and is not recoverable.

5. References: Policies, Instructions and Regulations

Community Owners, PCOs IOs, and end-users posting CUI, legacy FOUO, or PII to approved CUI communities must be familiar with and adhere to the following:

A. Freedom of Information Act (FOIA)

1. The "Freedom of Information Act" provides the most complete description of information that should be safeguarded from public or unauthorized exposure and release:
    a. Summary, video, FAQs, and list of 9 exemptions: https://www.foia.gov/faq.html
2. Generally, information uploaded into APAN is subject to access under the Freedom of Information Act.
3. APAN is the platform provider or Application Service provider and does not "own" content. Therefore, **all FOIA requests must be processed by the IO and/or PCO**, as content belongs to the command or organization that posted/published the information.

B. ISOO Policy for CUI and Categories Not Allowed on APAN

1. APAN is a U.S. DoD Information System, which aligns with the Information Security Oversight Office (ISOO) of the National Archives and Records Administration (NARA) regarding CUI
2. Details: https://www.archives.gov/cui/about
3. Policy/Guidance: https://www.archives.gov/cui/registry/policy-guidance
4. Category Marking List (click each category for details and marking/banner notes): https://www.archives.gov/cui/registry/category-marking-list
    a. All categories of CUI that might be shared within an APAN community must be documented on the request form; marking acronyms must be clearly indicated in the description field.
        i. Any questions from APAN staff about the types or amount of information as well as to what parties the information might be shared with need to be resolved by the PCO and/or IO within 5 business days, or requests will be denied pending further review
    b. The following CUI categories are explicitly **not allowed to be shared on the APAN platform**:
        i. Critical Infrastructure : CVI, CEII, ISVI, PCII, PHYS
        ii. Defense: DCNI, DCRIT, NNPI
        iii. Financial: FHFANPI, FSEC, NETW
        iv. Immigration: ADJ, ASYL, BATT, IVIC, PROT, RESD, VISA
        v. Intelligence: ID, IFNC, OPSEC
        vi. Law Enforcement: AIV, CHRI, CMPRS, FUND, INF, INV, JUV, LCOMM, LDNA, LFNC, LNSL, LSCRN, RWRD, SCV, SUB, TRACE, WHSTL
        vii. Legal: CHLD, CVIC, JURY, LPROT, LVIC, PRE, PRIOR, PRIVILEGE, WIT
        viii. NATO: NATO Restricted, NATO Unclassified
        ix. Nuclear: NUC, SGI, SRI, UCNI
        x. Patent: PSCEC
        xi. Privacy: CONTRACT, DREC, GENETIC, HLTH, MIL, PERS, PRIIG, PRVCY*, STUD
            1. *Certain exceptions for non-sensitive types of PII must be specifically identified, documented within the CUI request form, and approved by the APAN Capability Lead and the APAN Technical Director.

xii. Provisional: Homeland Security Enforcement Information, Information Systems Vulnerability Information - Homeland, Operations Security Information, Personnel Security Information, Physical Security - Homeland, Privacy Information, Sensitive Personally Identifiable Information

xiii. Tax: CONV, TAI, TAX, WDT

5. Limited Distribution / Dissemination (LIMDIS) Controls: https://www.archives.gov/cui/registry/limiteddissemination. Because information shared on APAN is accessible by anyone on the Internet with approved community membership, and because download destinations and devices cannot be controlled, CUI with **LIMDIS controls** other than REL TO [USA, LIST] **is prohibited.**

C. DoD Instruction 5200.48 and Policies Establishing DoD CUI Program

The DoD CUI Program website at https://www.dodcui.mil/Home/Policy/ contains resources for review:

1. Executive Order 13556, Controlled Unclassified Information: https://www.dodcui.mil/Portals/109/Documents/Policy%20Docs/EO%2013556%20CUI.pdf
2. 32 Code of Federal Regulations, Part 2002 (Implementing Directive): https://www.dodcui.mil/Portals/109/Documents/Policy%20Docs/CFR-2018-title32-vol6-part2002.pdf
3. **DoD Instruction 5200.48**, Controlled Unclassified Information (CUI): https://www.dodcui.mil/Portals/109/Documents/Policy%20Docs/DoDI%205200.48%20CUI.pdf

6. Additional Resources

Contact the APAN Help Desk to initiate a request or ask for assistance at any time:

1. Submit a ticket: https://www.apan.org/pages/support
2. Phone: (808) 472-7855
3. Knowledge Base (KB): https://community.apan.org/support