

All Partners Access Network



CUI Standard Operating Procedures for Community Owners

March 21, 2023

Document Version

All published versions of this document are approved by the APAN Technical Director and/or MPCO APAN Project Lead:

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

Contents

Document Version	2
1. Background	4
A. APAN Operational Environment and Security:	4
B. Terms	4
C. APAN Community Owner Guidelines and APAN Applications Governance	5
D. Considerations for determining if APAN is a suitable platform for hosting CUI	6
E. APAN Policy Remediating unapproved/unauthorized posting of CUI or PII	6
2. References: Policies, Instructions and Regulations	7
A. Freedom of Information Act (FOIA)	7
B. ISOO Policy for CUI and Categories Not Allowed on APAN	7
C. DoD Instruction 5200.48 and Policies Establishing DoD CUI Program	8
3. Responsibilities	8
A. PIM Responsibilities	8
B. IO Responsibilities	9
C. APAN Staff Responsibilities	9
4. General Procedures	10
A. Processing Request	10
5. Application-Specific Details	10
A. Microsoft SharePoint Sites	10
B. Verint Groups	11
C. Other APAN Capability Tools / Applications	11
6. Additional Resources	12

1. Background

Background details regarding sharing of Controlled Unclassified Information (CUI) on APAN: This document informs APAN users and community owners about overarching guidelines and Standard Operating Procedures for requesting approval to share CUI content within a community on the APAN platform. 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 APAN platform.

A. APAN Operational Environment and Security:

1. **Security Controls:** APAN is maintained under an approved Authorization to Operate (ATO) (NOV 2021) 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 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 on APAN.
2. **Constraints for CUI storage:** Storing CUI on the APAN platform should always be for **a specific operation or event with a defined start/end date**. APAN is not a records management platform, was never intended for long-term storage of CUI, and there are no overarching guidelines as of the date of this document for such purposes.
 - a. **Review of CUI published on non-CUI approved communities:** Regardless of the requirements behind choosing to store CUI on APAN, CUI requests must be approved by the APAN Technical Director. Instances involving 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 from the APAN platform. More information regarding how this is handled can be found in section 1E.
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 APAN Operational Environment, to include CUI communities. Approval for hosting CUI within an APAN community is granted by the APAN Technical Director (or designee).

If customers have additional technical questions about the status of the APAN environment and the types of security measures are in place, their concerns will be forwarded via Support Ticket to APAN government leadership. Keep in mind that APAN is a DoD Enterprise Information Sharing Service. To protect the status of our information systems, certain application & security details (including but not limited to versions of specific security services/tools in use, Authority to Operation (ATO) documents, Cloud Access Point (CAP) Waiver, or Risk Management Framework (RMF) Assessment and Authorization (A&A) process documentation) may only be shared with DoD personnel outside of the MPCO APAN Team upon approval of the APAN Technical Director.

B. Terms

1. **Community:** For the purpose of this document, the term “community” may refer to any site, group, portal, meeting room, or any type of collaborative workspace defined by any of the various APAN 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:** the standard label of “CUI” has been used for All Partners Access Network (APAN) communities requiring protection of Controlled Unclassified Information since March 2020. Previously, the standard DoD label of “For Official Use Only” (FOUO) was used as the generic title. The term CUI in this document refers to both the current and legacy versions of Controlled Unclassified Information within APAN.
4. **Portal Information Manager (PIM):** otherwise known as the primary Community Owner is responsible for membership, content and access attributes associated with the communities to which they are assigned as an owner or host on the APAN platform. They are required to complete the pre-requisites for community ownership identified in section 1.C.1-2 of this document.
5. **Information Official (IO):** The PIM’s 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 fill the role of IO; any Flag/General Officer (FOGO), Senior Executive Service (SES) Civilian or Staff Directors are 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 PIM may be one and the same person; regardless, 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 an APAN community.

C. APAN Community Owner Guidelines and APAN Applications Governance

1. Per SOPs, anyone with privileges as an APAN Community Owner or Host is required to do the following in compliance with security policies for the protection of CUI data:
 - a. Review the APAN Community Owner Guidelines:
<https://community.apan.org/support/m/info/139431>
 - b. Review the APAN Applications - Generalized Governance for End-Users:
<https://community.apan.org/support/m/info/262852>
 - c. Download a copy of the blank APAN "Community Owner Acknowledgement" (COA) form:
<https://community.apan.org/support/m/info/139434>
 - d. Review, fill out and sign the APAN COA Form with your CAC, PIV or DoD/GOV digital certificate and attach/upload the digitally signed file to a new entry at
<https://wss.apan.org/s/ASPR/Lists/Completed%20Forms/AllItems.aspx>
2. Application-specific Community Owner Training is available at the following link or upon request:
 - a. <https://community.apan.org/support/p/apanu>
3. COA/CUI forms and communications involving new/additional (or transfer of) community owners will be maintained by APAN staff; if updates to policy and/or forms occur, APAN staff may request owners to complete new form(s).

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

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

1. Frequently, situations dictate that CUI be shared with participants who do not have access to the NIPRNet or other Public Key Infrastructure (PKI)-protected systems (e.g., coalition unclassified exercises, multinational unclassified events, etc.). In many operationally intense situations such as Humanitarian Assistance/Disaster Relief (HADR) or Defense Support of Civil Authorities (DSCA) operations and crisis response situations, NIPRNet is not physically available and the only means for information sharing exist via commercial Internet via an organic infrastructure (e.g., Wi-Fi or Mobile Broadband network connectivity). In these instances, sharing CUI information with specified partners takes precedence over denying this service because NIPRNet is not available.
2. APAN is designed to prioritize information sharing over information protection. However, even in the case of HADR/DSCA, crisis-response, or emergency EVENTS WHICH REQUIRE CUI PROTECTION, CUI is not authorized to be uploaded into APAN unless specifically approved by the APAN Technical Director.
3. It is the sole responsibility of command leadership (e.g., appointed IO) to make the final determination regarding whether or not they would like to request approval to share CUI on their respective APAN community. APAN contractor staff may only confirm stated policy/guidelines and will not make any suggestions, recommendations, or advisements about whether a particular command should use the APAN platform to share any types of CUI. Any questions or requests for clarification about platform stipulations may be resolved by APAN government leadership.
4. PII is not allowed on APAN except in limited cases when the PII shared is commonly available professional contact information like phone numbers and email. Each case must be requested via the APAN CUI request process and approved by the APAN Technical Director.

E. APAN Policy Remediating unapproved/unauthorized posting of CUI or PII

System administrators will randomly run security check to identify CUI, legacy FOUO or PII content uploaded to unapproved communities. When such content is identified, the KM's will be notified. The KM's will then notify the community owners via an APAN ticket and inform the owners they have 24 hours to remove the content. If that content is not removed within 24 hours, the KM's will delete any CUI, legacy FOUO or PII content and such content will not be restored.

1. For security reasons, APAN administrators may remove content for anything 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.C of this document; instances involving 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 from the APAN platform.

2. References: Policies, Instructions and Regulations

Community Owners, Portal Information Managers (PIMs), Information Officials (IOs) and any end-users posting CUI, legacy FOUO, or PII to approved CUI communities on the APAN platform 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. As a general rule, information uploaded into APAN is subject to access under the Freedom of Information Act (FOIA).
3. APAN is the platform provider or Application Service provider and does not “own” content. Therefore, **all FOIA requests must be processed by the Information Owner and/or Portal Information Manager**, 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 List (click each category for details and marking/banner notes):
<https://www.archives.gov/cui/registry/category-list> ; or table at <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 PIM 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 Technical Director.
Contact your APAN KM for additional required form(s)/documentation.
- 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> . Due to the fact that information shared on APAN may be accessible by anyone on the Internet with approved community membership and there is no way to guarantee or control where or to what device(s) end-users may download such data to, any CUI with **LIMDIS controls** other than REL TO [USA, [LIST](#)] **is not allowed to be shared on the APAN platform.**

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>

3. Responsibilities

A. PIM Responsibilities

1. PIMs are Community Owners responsible for management of and access to CUI posted within their community; responsibilities include, but are not limited to:
 - a. Complete documentation within the initial request for the APAN CUI form, including CAC/PIV signature
 - b. Adhere to guidance stated in section 1.C of this document and complete APAN-administered “Community Owner Training” acquainting them with application-specific PIM responsibilities
 - c. The PIM is accountable for all community membership/access requests and for all content posted to the community
 - i. Reminder: Any user who has been granted elevated Community Owner or Host privileges must **also** sign and submit a (COA) form
 - d. Strictly enforce least privileged access to all CUI documents and information
 - e. Restrict access to CUI to only authorized users as determined by the IO
 - f. Make every attempt possible to validate the user, user account name and “need to know” before granting access to CUI
 - g. Ensure posted CUI content is limited to those items only relevant to the mission and posted sparingly

- h. Perform reviews to validate only authorized CUI is posted and purge any CUI deemed no longer relevant to the operational situation
- i. If any CUI is posted without authorization, the PIMs shall be responsible for removing it from the APAN web server within 24 hours of identification
 - ii. If combined unclassified information elements are determined to be potentially classified, the PIM must purge the most sensitive information set and notify the Information Official
- j. Notify APAN staff regarding any new sub-sites/sub-groups created underneath an approved CUI community so that banners are properly activated for nested communities
- k. Following the end of a qualifying exercise, mission, project, conference, or other event in which CUI is utilized, the PIM must notify the APAN Help Desk to permanently delete the community
- 2. PIMs must respond to requests for information from APAN staff and/or community members
 - a. Providing guidance about CUI for community members and anyone posting content within a community is the responsibility of the PIM and/or IO for that respective community.

B. IO Responsibilities

- 1. Review and complete documentation for the APAN CUI 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 PIM.

C. APAN Staff Responsibilities

- 1. KMs:
 - a. Process requests: review documentation received from customer including purpose/description, ensure all fields are filled in properly & verify CAC/PIV signatures, respond back to customer when decision is made by the APAN Technical Director (or designee) to approve/deny request, and update documentation in the APAN tracking list of all CUI communities.
 - b. Activate banners for initial (parent or top-level) group(s)/site(s) as well as any subsequent requests for CUI banner activation within sub-sites/sub-groups created under the same parent community
 - c. Respond to and maintain communication with the customer regarding any safeguard concerns for content or community membership that requires action from the customer or upon notification from APAN Cybersecurity analyst(s)
 - d. Delete expired communities; otherwise, process renewal requests for communities that continue to be active or have indicated within their previous request form that they require a renewal
 - e. Delete unapproved CUI or PII content that was not removed within 24 hours as recommended by System administrators.
- 2. APAN Technical Director (or designee) and/or MPCO APAN Project Lead: Review and sign for final approval (or respond to indicate denial/non-concur) for APAN CUI community requests
- 3. APAN staff members will **not** provide any advisement, recommendations, suggestions, or guidance regarding whether or not any specific CUI should or should not be posted to an approved CUI community, other than confirming what was documented on the approved request form.

4. General Procedures

A. Processing Request

1. The customer must submit an APAN CUI Request Form identifying the Information Official (IO), Portal Information Manager (PIM) - otherwise known as Primary Community Owner - describe membership & attributes associated with Community of Interest (COI), and complete APAN Community Owner Training
2. Link to current form: <https://community.apan.org/support/m/info/139432>
 - a. Both the PIM and IO must sign the form with their CAC/PIV digital certificate
 - b. “End Date” should be **no longer than 2 years from request date**; check renewal option if needed
3. The APAN KM will review the form, make any minor changes as needed and/or coordinate with the customer if additional documentation is needed to clarify the request
4. The APAN Lead KM will forward requests to the APAN Technical Director (or designee) and/or MPCO Project Lead on a weekly basis
5. Once the previous requirements are met and authorization is approved by the APAN Technical Director, APAN administrators will take action to enable the group to CUI, and a banner will automatically be displayed at the top of the group indicating that it has been officially approved for storage of CUI.
 - a. The community will be permanently designated as CUI and all changes to group or site settings related to CUI must not be modified after-the-fact
 - b. If there is a need to also share unclassified-only information with a different group of users (using different permissions groups or access control measures), the customer must initiate a request to create a separate community for such purposes
 - c. Non-CUI groups or sites must not be created as a sub-community of a parent group or site approved for CUI. Once a community is approved for CUI, all sub-communities to that community shall also be CUI. Non-CUI sub-communities are NOT permitted under an approved CUI community.
6. The APAN KM will notify the customer via Support Ticket and update internal documentation.
7. Within 30 days after the “End Date”, the community (and any sub-communities, including any and all content/membership and nested communities) will be permanently deleted unless the customer has indicated they wish to renew; if so, a new request form will be processed for the renewal
 - a. The PIM needs to be cognizant of when CUI approval status is approaching expiration; if the current Community Owner(s), PIM, or IO does not respond to email requests from APAN staff to renew their APAN CUI status within 10 business days, the CUI community will be permanently deleted
 - b. APAN admins will delete CUI communities if they have been inactive (no content posted) > 1 year

5. Application-Specific Details

A. Microsoft SharePoint Sites

1. Search and Offline availability settings for the site and Anonymous Access must be turned off
2. Verify there is no “Anonymous”, “NT Authenticated”, “All authenticated users”, “All Windows users”, or similar generic, enterprise-wide directory access enabled for any elements of the site (including unique list, library, or document-specific permissions)
3. Application controls are in place to prevent users from setting “alerts” on lists or libraries, which will prevent any CUI or attachments from being emailed to end-users

4. If any permissions/controls appear to have been modified or circumvented by site owners that would allow for the possibility of unauthorized access, APAN staff administrators will take steps to safeguard information on the platform:
 - a. PIM, IO, and any other Community Owner(s) will be notified to take immediate steps to correct the situation and/or may be required to attend remedial training
 - b. The APAN Technical Director will be informed regarding any repeated violations for the community, which may result in the customer losing the privilege of storing/managing data on the APAN platform; a new PIM may need to be selected by the command/organization

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. A warning will be displayed before files can be downloaded.
 - a. This removes the actual post that is normally generated when members of a group subscribe to a Blog or Forum, and instead inserts words that advise members they must log in to APAN and return to the community to read posted content
3. If any application-specific permissions/controls appear to have been modified or circumvented by group owners/managers that would allow for the possibility of unauthorized access to Blogs, Forums, Wikis, or Media Galleries within the group, APAN staff administrators will take steps to safeguard information on the platform:
 - a. PIM, IO, and any other Community Owner(s) will be notified to take immediate steps to correct the situation and/or may be required to attend remedial training
 - b. The APAN Technical Director will be informed regarding any repeated violations for the community, which may result in customer losing the privilege of storing/managing data on the APAN platform; a new PIM may need to be selected by the command/organization

C. Other APAN Capability Tools / Applications

1. For all other tools/platforms such as Adobe Connect rooms, Arc GIS portals, or Chat rooms which may be noted on the approved CUI request form, it is the responsibility of the Community Owner or Host to inform users that CUI is authorized
 - a. Community Owners/Hosts must diligently review access permissions for any additional information exchange capabilities associated with their APAN community, complete training, and take steps to correct any access-related problems identified by APAN staff when notified.
 - b. In accord with guidance listed in this document at section 1.C.1.b, **no recording at the CUI level will be permitted using Adobe Connect**
 - c. **Hosts must confirm access settings for Adobe Connect rooms at CUI level and verify that the “Anyone who has the URL for the meeting can enter the room” option is NOT enabled.** List of access settings:
 - i. Registered users may enter the room: **best security setting**. Hosts are required to approve APAN account members who are requesting to join the meeting
 - ii. Account Members may enter the room: Allowed, but not as secure and not recommended, since anyone with an APAN account can join without being vetted/approved to be in the meeting.

- iii. Accepted guests may enter the room: Allowed, but not recommended, as hosts might not be able to confirm true identity of unauthenticated “guests” before approving them to join.
 - iv. Anyone who has the URL for the meeting can enter the room (this means the room is fully “public” and allows anyone on the Internet access to the room and uploaded content without having ever been vetted/approved by a host at any time): **Do not ever use this setting for CUI!**
- 2. Community owners may contact the APAN Help Desk to request details and instructions for creating an HTML header/banner for use on an as-needed basis
 - 3. Community owners may contact the APAN Help Desk to receive guidance on how to use APAN tools to export content that the Owner wishes to keep on his/her own local network or any information system(s) external to the APAN platform
 - a. APAN staff will **not** export data on behalf of customers with the exception of specific SharePoint document library content; such requests must be submitted by Community owner(s) (or IO) at least 10 business days prior to 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

6. Additional Resources

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

- A. Web form (create at ticket): <https://community.apan.org/support/p/contact>
- B. Phone: (808) 472-7855 / DSN 315-472-7855
- C. Email: support@mpe.apan.org
- D. Knowledge Base (KB): <https://community.apan.org/support>