Network Account Request Form

Instructions for Completion

This form is designed to be completed as an electronic form in accordance with DoDI 7750.07. Supervisors will provide the requester supervised access to prepare and sign the form using their Common Access Card (CAC). If the account holder is not eligible for a CAC then print this form and physically sign. Using either a Digital Sender or Unit Perms scanner, save this form as a PDF, and submit as appropriate. If you are unable to accomplish this task then call the J6 Help Desk for instructions. **All three (3) pages must be received by the J6 Help Desk. Page 1 and 2 must be initialed. Section 3 must be signed by the submitter. Section 4 must be singed by a person with an active Network account. Failure to submit all three (3) pages, sign section 3, and have section 4 completed by a person with an active account is grounds for denial. Completed forms can be sent to the J6 Service Desk via email to ng.ca.caarng.mbx.j6-service-desk@mail.mil or by fax (916) 854-3018.**

Section 1 – Acceptable use Policy and Acknowledgements

Network access is a revocable privilege, subject to the standards of conduct, rules and regulations set forth in applicable Joint Ethics, DoD, and Army regulations. The California National Guard Network is part of the larger DoD Unclassified but Non-secure Internet Protocol Router Network (NIPRNet). These networks are accredited to operate at the UNCLASSIFIED level only, per Joint Ethics Regulation, DOD 5500.7-R, AR 25-1, AR 25-2, and other applicable DOD, DA, Army Task orders, and local policies.

Department of Defense (DoD) Mandated Requirements:

By signing this document, you acknowledge and consent that when you access Department of Defense (DoD) information systems:

* You are accessing a U.S. Government (USG) information system (IS) (which includes any device attached to this information system) that is provided for U.S. Government authorized use only.

* You consent to the following conditions:

o The U.S. Government routinely intercepts and monitors communications on this information system for purposes including, but not limited to, penetration testing, communications security (COMSEC) monitoring, network operations and defense, personnel misconduct (PM), law enforcement (LE), and counterintelligence (CI) investigations.

o At any time, the U.S. Government may inspect and seize data stored on this information system.

o Communications using, or data stored on, this information system are not private, are subject to routine monitoring, interception, and search, and may be disclosed or used for any U.S. Government-authorized purpose.

o This information system includes security measures (e.g., authentication and access controls) to protect U.S. Government interests--not for your personal benefit or privacy.

o Notwithstanding the above, using an information system does not constitute consent to personnel misconduct, law enforcement, or counterintelligence investigative searching or monitoring of the content of privileged communications or data (including work product) that are related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants. Under these circumstances, such communications and work product are private and confidential, as further explained below:

- Nothing in this User Agreement shall be interpreted to limit the user's consent to, or in any other way restrict or affect, any U.S. Government actions for purposes of network administration, operation, protection, or defense, or for communications security. This includes all communications and data on an information system, regardless of any applicable privilege or confidentiality.

The user consents to interception/capture and seizure of ALL communications and data for any authorized purpose (including personnel misconduct, law enforcement, or counterintelligence investigation).

However, consent to interception/capture or seizure of communications and data is not consent to the use of privileged communications or data for personnel misconduct, law enforcement, or counterintelligence investigation against any party and does not negate any applicable privilege or confidentiality that otherwise applies.

- Whether any particular communication or data qualifies for the protection of a privilege, or is covered by a duty of confidentiality, is determined in accordance with established legal standards and DoD policy. Users are strongly encouraged to seek personal legal counsel on such matters prior to using an information system if the user intends to rely on the protections of a privilege or confidentiality.

_____
Initial

- Users should take reasonable steps to identify such communications or data that the user asserts are protected by any such privilege or confidentiality. However, the user's identification or assertion of a privilege or confidentiality is not sufficient to create such protection where none exists under established legal standards and DoD policy.

- A user's failure to take reasonable steps to identify such communications or data as privileged or confidential does not waive the privilege or confidentiality if such protections otherwise exist under established legal standards and DoD policy. However, in such cases the U.S. Government is authorized to take reasonable actions to identify such communication or data as being subject to a privilege or confidentiality, and such actions do not negate any applicable privilege or confidentiality.

- These conditions preserve the confidentiality of the communication or data, and the legal protections regarding the use and disclosure of privileged information, and thus such communications and data are private and confidential. Further, the U.S. Government shall take all reasonable measures to protect the content of captured/seized privileged communications and data to ensure they are appropriately protected.

o In cases when the user has consented to content searching or monitoring of communications or data for personnel misconduct, law enforcement, or counterintelligence investigative searching, (i.e., for all communications and data other than privileged communications or data that are related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants), the U.S. Government may, solely at its discretion and in accordance with DoD policy, elect to apply a privilege or other restriction on the U.S. Government's otherwise-authorized use or disclosure of such information.

o All of the above conditions apply regardless of whether the access or use of an information system includes the display of a Notice and Consent Banner ("banner"). When a banner is used, the banner functions to remind the user of the conditions that are set forth in this User Agreement, regardless of whether the banner describes these conditions in full detail or provides a summary of such conditions, and regardless of whether the banner expressly references this User Agreement.

California National Guard (CNG) Policy Enhancements (AR 25-2 & Local Policies) :

a. Supervisors are responsible to be aware of their subordinates' usage through casual observation and monitor their compliance with all DOD, Army, and Local policies. (Policy Memo 07-08)

b. I will not process classified information on the CA Network, a NIPRNET communications system (para 4-6k).

c. I will not use Government Information Systems if my access to classified materials has been revoked or am aware of my Favorable Background being returned with derogatory remarks (para 4-14).

d. I will not connect non-government devices, information systems or Personal Electronic Devices to the NIPRNet (para 4-5(a)6).

e. Users are prohibited from bringing personal computers on CA National Guard facilities.

f. I will not share my user name and password or Common Access Card and PIN to individuals not granted access. This includes modem, VPN, and Citrix remote access capabilities. (para 4-5(a)8).

g. Email services are provided for use in brief communications related to official government business and approved uses per J6 Policy Memorandum. (para 4-5(r)(6)).

h. I will limit the number of email recipients on all message traffic to the minimum necessary to accomplish the task or mission. (J6 Local Policy).

i. I will not use personal email or telecommunications devices to conduct official government business (para 4-5(m)1).

j. I will not send Personally Identifiable Information (PII), For Official Use Only (F.O.U.O.), Law Enforcement Sensitive (L.E.S.), or Classified information to personal email addresses. (para 4-5(m)1).

k. In order to protect the network from viruses and other illegal activities, certain content is blocked at the national and local level. Access to the following content is prohibited:

- Pornography
- Obscene Materials (Adult and Child)
- Copyright Infringement Sites
- Commercial Blogs
- Gambling Sites
- Hate speech and Racism sites
- Dating sites
- Commercial Chat Rooms

l. The J6 internet usage policy prohibits users from maintaining web content for unofficial activities while using government resources without written JAG / J6 Approval. Examples include the following types of technologies include but are not Limited to:

_____
Initial

- Blogs
- Wikis (commercial software used to create collaborative websites, power community websites)
- Unofficial Web Sites
- File sharing sites
- Commercial VPN and other applications designed to provide remote access to government systems.
- Scripts, programs, or other executable content designed to execute on an information system.
- Video or Audio Content to include streaming media, videos, music, news, or editorial commentary.

m. I am allowed to utilize the internet for participation in military and civilian education pursuits, in the course of conducting functions of my job, seeking employment, and for general research which do not conflict with items j or k above.
n. I will not maintain commercial web sites, visit social networking sites, blogs, or commercial chat rooms. (Policy Memo 07-08)
o. Use of government information systems to access unlawful or unauthorized activities such as file, data, or other content sharing that is protected by Federal or State Law, to include copyright. (para 4-5)
p. Individual supervisors are responsible to counsel their subordinates on personal usage times, appropriate length of use and activities. Refer to Policy Memo 07-08 and items f-n of this document for specific guidelines.
q. I will not use government storage systems to store personal media to include (but not limited to) music, videos, and pictures.
r. Personal use is defined as all activities conducted on government furnished information systems and circuits where the usage is not directly related to the conduct of official government business. (Policy Memo 07-08).

Remote Access Addendum:

I understand that the term remote access refers to any capabilities or permissions granted that allow access to official CA National Guard resources from a civilian external network connection (e.g. home, hotel, etc.). I acknowledge that I may only access Virtual Private Network (VPN) connections using a Government Furnished computer, approved by the CA J6. Citrix access may be accessed from a non-government furnished computer as long as the use verified all current patching and anti-virus patches are applied.

Section 2 – Account Requester

Failure to complete Section 2 and obtain approval from an individual with an active Network Account are grounds for denial. Air Force personnel must submit proof of a Local Records Review with their account request. Fax or email the completed form to the J6 Service Desk at (916) 854-3018 or **ng.ca.caarng.mbx.j6-service-desk@mail.mil** **Note: All three pages must be submitted.**

Last Name	**First Name**	**AKO Email Address:** **AKO user name cannot exceed 20 characters**	**Rank:**
Employment Status: ☐ Full-Time ☐ M-Day ☐ SDF ☐ Other Volunteer Group		**Full-Time Classification (check 1):** ☐ St Civ Svc ☐ Contractor ☐ AGR ☐ SAD ☐ Mil Tech ☐ Civ Tech ☐ Other	**Business Phone** (area code and number)
Enter EDIPI Number from CAC (e.g.Smith.William.A.**129395353**)			**Last 4 SSN** (xxxx)

Section 3 - Account Holder Acceptance

By signing this document, you acknowledge you have read pages 1 through 3 and understand the policies, procedures, and guidelines set forth and provide your consent as a condition of your access to Department of Defense Information Systems. If you need assistance completing this form, please contact your supporting J6 office at (866-CNG-DOIM) for assistance. Failure to accept this agreement is grounds for account denial.

Printed Name	**Signature**	**Date**

Section 4 – Sponsor Verification

By signing this document you have personally verified the requester listed above has a valid Common Access Card (CAC), has a valid requirement for Network access, and has completed the entire application truthfully and accurately. You further verify that the requester has read and understands the policies, procedures, and guidelines set forth in this application. You also certify that you have an active Network Account.

Printed Name and Rank	**Signature**	**Date**

Section 5 – Verification (Internal Use Only)
(To be completed by JFHQ Security Branch or Wing Information Security Specialist)

By signing this document, you acknowledge you have personally verified the requester listed above has a favorable background (as per local published policy). All requests will be forwarded for approval to the JFHQ Security Branch for final approval.

Printed Name and Rank	**Signature**	**Date**