These step-by-step instructions are intended to help you acquire access to the JAGCNet managed information systems.

NOTE: SUBMITTED FORMS NOT PROPERLY COMPLETED WILL BE RETURNED.

To complete the form, follow the steps below:

TYPE OF REQUEST:

- Initial: New user accounts and accounts that need to be re-established due to deletion.
- Modification: Changes to an existing account.
- Deactivate: Delete the user account.
- User ID: This is no longer required.

DATE: Enter the date of the request. (All dates must be entered in YYYYMMDD format.)

NOTE: DD2875 must be dated within 30 days of submission date. Submitted forms dated over 30 days from day of submission will be rejected.

SYSTEM NAME: Ensure the system name matches the system you are requesting.

LOCATION: Please fill in with complete information

PART I and PART II (*Blocks to be completed by **Requestor***):

1. **Name**: Last Name, First Name, and Middle Initial.
2. **Organization**: Enter full unit name
3. **Office Symbol/Department**: Enter unit office symbol or department name.
4. **User's Phone Number**: Check DSN (Defense Switched Network) or Commercial and then enter the appropriate number including area code for commercial numbers.
5. **User's Official Email Address**: Enter official e-mail address.
6. **Job Title & Grade/Rank**: Enter job title and grade/rank.
    - Contractors enter "CTR" as the grade/rank.
7. **Official Mailing Address**: Enter official mailing address.
8. **Citizenship**: Select US or FN (Foreign National) or OTHER as appropriate.
9. **Designation of Person**: Select MILITARY, CIVILIAN or CONTRACTOR.
10. **IA Training and Awareness Certification Requirements**: Check the – "I have completed Annual Information Awareness Training." block and *enter the Date of Training in the stated format*. Check ATCTS to obtain training date. (** **The IA date can be no more than one year prior to the date of submission.** **)
11. **User Signature:** Prior to signing the form, the user must ensure that blocks 1-10 & 13 are filled in completely.
12. **Date:** Enter date in YYYYMMDD format.

16a. **Access Expiration Date (Contractors only):** Enter the date that access is to be terminated. Contractors must specify company name, contract number, and expiration date. Use **block 21** if additional space is required. Contractor accounts expire on the contract expiration date. An updated DD 2875 is required to prior to the current contract expiration date to keep the account active.

*****User Portion is now complete*****

***** Ensure you have signed the form in block 11 *****

Please save the form using the naming convention below and send to your supervisor for further processing. [System] – [Last], [First] – DD-2875.pdf (e.g. Doe, John – DD-2875.pdf)

PART II (*Blocks to be completed by* ***Supervisor***):

13. **Justification for Access:** Verify the requestor's justification. This is the **PURPOSE** of the system access required and the access being requested. This entry **CANNOT** be a generic statement, such as "Access required to perform job duties."

    Example of a valid justification: *As a legal administrator, I need to be able to perform legal duties within the JAGCNet information system, to include:* ***(enter job duties here).***

14. **Type of Access Required:** Check "Authorized". "Privileged" access is not granted to users outside the JAGCNet Information Technology Division.

15. **User Requires Access to:** Check appropriate box.

16. **Verification of Need to Know**: This block should be checked, acknowledging supervisor's verification that the requestor has a valid need for access to the system.

    NOTE: Supervisor will assume all risks associated with the misuse of the information/contents of a JAGCNET account on this information system.

17. **Supervisor's Name:** Enter Supervisor name.
17a. **Supervisor's E-mail Address:** Enter e-mail address.
17b. **Phone Number:** Enter phone number.
17c. **Supervisor's Organization/Department:** Enter organization/department.
17d**. Supervisor's Signature:** Must be a digital signature.
17e. **Date:** Enter the date the document was signed. Must match date of digital signature.
21. **Optional Information**: Delete application(s) that access is unneeded. Only applications which are required for the performance of the user's job duties should be listed here. If you do not require access to any JAGCNet applications, please state that.

*****Supervisor Portion Complete*****
***** Ensure you have signed in block 17d *****

Part III needs to be filled out by the Information Owner, Security Manager, ISSO to complete the form. Please read all requirements below:

NOTE: Please use local security manager to validate security requirement in boxes 22-26.

The below acknowledgement and consent apply to all users who access a JAGCNet information system:

ACKNOWLEDGEMENT AND CONSENT

1. Acknowledgement. By signing the user agreement, the user acknowledges and consents that when they 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.

2. Consent.

a. You consent to the following conditions:

(1) 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.

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

(3) 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.

(4) 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.

b. 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.

(1) 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.

(2) 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 or 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.

(3) 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.

(4) 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.

(5) The 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.

(6) 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 or seized privileged communications and data to ensure they are appropriately protected.

(7) 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, (that is, 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.

(8) 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.

PART II

INFORMATION SYSTEM ACCESS

1. Understanding. The user understands that they have the primary responsibility to safeguard the information contained on the system being accessed from unauthorized or inadvertent modification, disclosure, destruction, denial of service, and use. Any use of Army Information Technology (IT) is made with the understanding that the user will have no expectation as to the privacy or confidentiality of any electronic communication, including minor incidental personal uses.

2. Access. DoD policy states that Federal Government communication systems and equipment (including Government owned telephones, facsimile machines, electronic mail, internet systems, and commercial systems), when use of such systems and equipment is paid for by the Federal Government, will be for official use and authorized purposes only. Official use includes emergency communications and communications necessary to carry out the business of the Federal Government. Authorized purposes include brief communications by employees while they are traveling on Government business to notify family members of official transportation or schedule changes. Authorized purposes can also include limited personal use established by appropriate authorities under the guidelines of the DoD Regulation 5500.7-R, para. 2-301 "Joint Ethics Regulation."

a. Internet Access. Internet access is intended primarily for work related purposes.

(1) The user will not circumvent any filters or blocks to gain access to restricted sites.

(2) If denied access to a particular website, needed for official or authorized use, the user will follow procedures on the "blocked website" notification to request the site be unblocked.

(3) The user will not use Army IS for activities that are illegal, inappropriate, or offensive to fellow employees or the public. Such activities include, but are not limited to: hate speech, or material that ridicules others on the basis of race, creed, religion, color, sex, disability, national origin, or sexual orientation.

(4) The user will not inflict harm through the use of electronic communication – the transfer of information (signs, writing, images, sounds, or data) transmitted by

computer, phone, or other electronic device. Examples include harassment, bullying, hazing, stalking, discrimination, retaliation, or any other types of misconduct that undermines dignity and respect.

b. Email.

(1) The user will adhere to the email practices as outlined in AR 25-1 or your local command.

(2) The user will properly report chain email, spam, and virus warnings by following the reporting procedures outlined by your local command.

(3) The user will not provide personal or official information if solicited by email

(4) The user will not use personal, commercial email to conduct official government business.

(5) The user will not auto-forward email from official government email to a commercial or personal email accounts.

3. Revocability. Access to Army resources is a revocable privilege and is subject to content monitoring and security testing. If the user knowingly threatens or damages an Army Information System (IS) or communications system (for example, hacking or inserting malicious code or viruses) or participates in unauthorized use of Army network(s), the user will have their network access suspended or terminated.