National Industrial Security Program
Enterprise Mission Assurance Support Service
User Account Request Guide

DEFENSE COUNTERINTELLIGENCE AND SECURITY AGENCY

National Industrial Security Program Authorization Office

Version 1.0

14 March 2022

TABLE OF CONTENTS

1 INTRODUCTION

1.1 BACKGROUND

The Enterprise Mission Assurance Support Service (eMASS) is a government-owned, web-based application with a broad range of services for comprehensive fully integrated cybersecurity management. The Defense Information Systems Agency (DISA) manages eMASS's core functionality and established the National Industrial Security Program (NISP) instance of eMASS for cleared Industry.

The NISP eMASS is used to automate the Risk Management Framework (RMF) process. This instance is only for cleared contractors under the cognizance of the Defense Counterintelligence and Security Agency (DCSA) and assigned to a Commercial and Government Entity (CAGE) Code.

This guide is designed to assist cleared contractors with completing the following NISP eMASS user account prerequisites:

- DISA eMASS Computer Based Training (CBT)
- Cyber Awareness Challenge (CAC) training
- DCSA System Authorization Access Request (SAAR)
- NISP eMASS User Registration

1.2 REQUIREMENTS

As stated above, the NISP instance of eMASS is only for cleared contractors under the cognizance of the DCSA. A NISP eMASS user account is used to maintain and oversee the system security program. In order to perform these duties, an individual is required to have a security clearance. The NISP instance of eMASS is not approved for storing classified information. However, details of systems authorized and seeking authorization for classified processing are maintained in the application. A Facility Security Officer (FSO) and/or member of the Key Management Personnel (KMP) is required to endorse a NISP eMASS user account request. By endorsing the request, the FSO and/or member of the KMP is stating that the individual is able to have a NISP eMASS account and perform system security program responsibilities. One of those responsibilities is to be appropriately cleared.

Prior to approving a NISP eMASS user account, the DCSA will confirm that the cleared contractor is assigned to a CAGE Code. The CAGE Code must have a facility clearance (FCL) and approved safeguarding. Safeguarding refers to a facility's ability and authorization to safeguard classified information. All facility information is validated via the National Industrial Security System (NISS).

Cleared Industry users requiring access to the NISP eMASS instance must also have a Department of Defense (DoD) Public Key Infrastructure (PKI) certificate on an External Certification Authority (ECA) or Common Access Card (CAC). Cleared Industry contractors should only use issued DoD credentials associated with their current NISP responsibilities.

2 TRAINING PREREQUISITES

2.1 EMASS COMPUTER BASED TRAINING

Industry users must complete the DISA eMASS Computer Based Training (CBT) prior to being granted access to the NISP eMASS. The DISA eMASS CBT is hosted on the RMF Knowledge Service site. In order to access the site and complete the eMASS CBT, Industry will perform the following actions:

1. Access the RMF Knowledge Service site: https://rmfks.osd.mil/rmf/Pages/default.aspx
2. Click the LOGIN button.
3. Click on DoD ECA Certificate.
4. The SPONSORSHIP REQUEST FORM page will appear. Industry users will need to get sponsored by their assigned Information Systems Security Professional (ISSP). Complete the form as follows:
    a. Enter the user information in the TOP PORTION
    b. Choose the Email or Name option for the drop down.
    c. Enter the assigned ISSP email or name.
    d. Click Find Sponsor.
    e. Choose the Sponsor email or name.
    f. Submit the form.
    g. A sponsorship request received confirmation will appear.
5. The assigned ISSP will receive the sponsorship request for approval. The ISSP will access the RMF Knowledge Service site and approve the pending request. *Note: It is recommended that Industry contact their assigned ISSP and inform them of the sponsorship request.*
6. Once sponsorship is approved by the assigned ISSP, Industry users will be able fully access the RMF Knowledge Service site.
7. Complete the eMASS CBT: https://rmfks.osd.mil/rmfresources/eMASS/CBT/index.html. The CBT can also be found in the "eMASS" portion of the "Help and Resources" section on the page "What is eMASS?". The eMASS CBT takes approximately 2 hours to complete and must be completed in one session.
8. At the end of the final exam, the certificate will display on the screen. Save a copy of the certificate. Users may screenshot or print to Portable Document Format (PDF). *Note: The site does not save your certificate of completion. Training certificate completion dates cannot be greater than one year of the account request.*

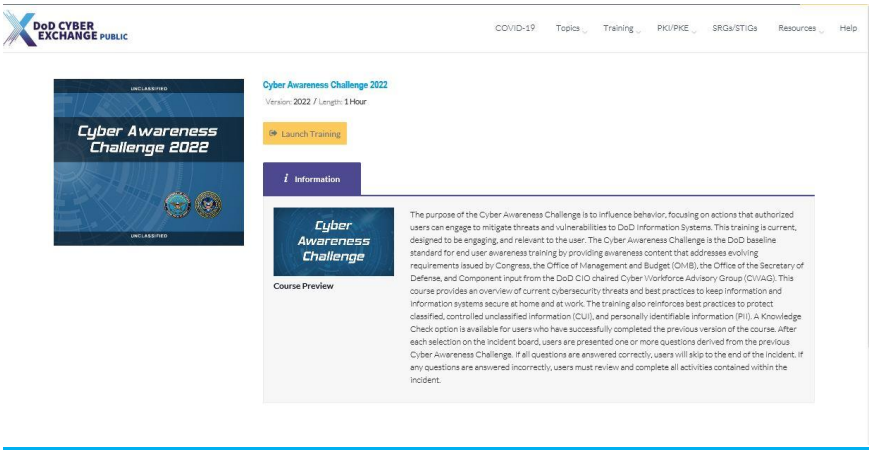
DCSA does not own/manage the RMF Knowledge Service site. If Industry users are having application issues, please contact the RMF Technical Inquiries Team at osd.pentagon.dod-cio.mbx.support-rmfknowledgeservice@mail.mil.

2.2 CYBER AWARENESS CHALLENGE TRAINING

Industry users must complete the Cyber Awareness Challenge training prior to being granted access to the NISP eMASS. In order to complete the training, Industry will perform the following actions:

1. Access the training on the DoD Cyber Exchange Public site: https://public.cyber.mil/training/cyber-awareness-challenge/

2. Select "Launch Training".



3. Select "Start New Session".

4. After completing the training, save a copy of the certificate of completion. *Note: The site does not save your certificate of completion. Training certificate completion dates cannot be greater than one year of the account request.*

DCSA does not own/manage the DoD Cyber Exchange Public site. If Industry users are having application issues, please follow the guidance here: https://public.cyber.mil/help/.

3 SYSTEM AUTHORIZATION ACCESS REQUEST

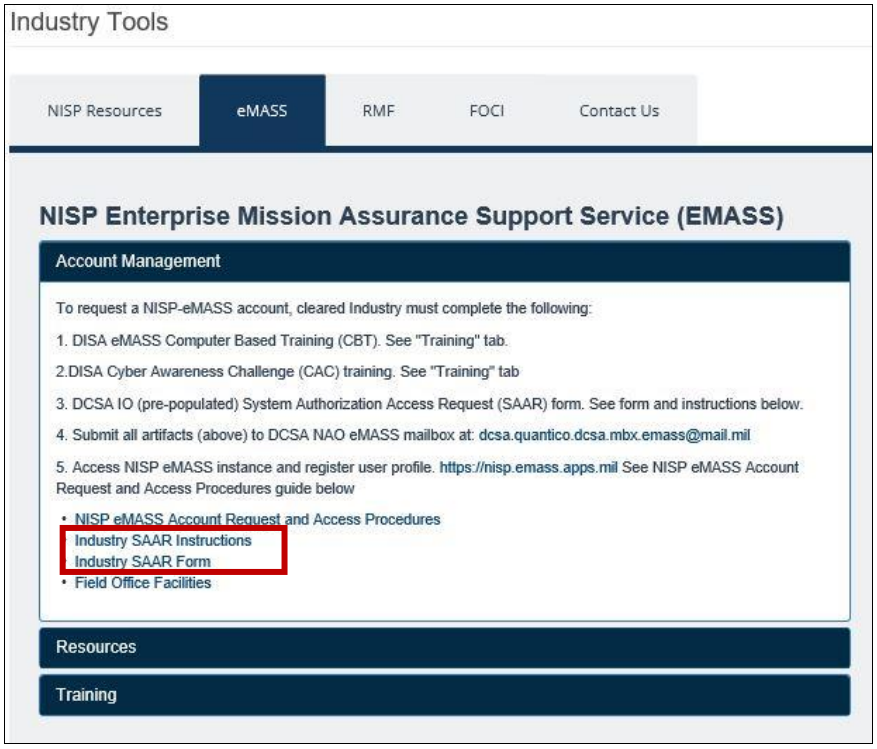
Industry users must complete the DCSA System Authorization Access Request (SAAR) prior to being granted access to the NISP eMASS. Industry will perform the following actions:

1. Go to the following DCSA site: https://www.dcsa.mil/mc/ctp/tools.

    a. Select the eMASS Tab

    b. Select Account Management

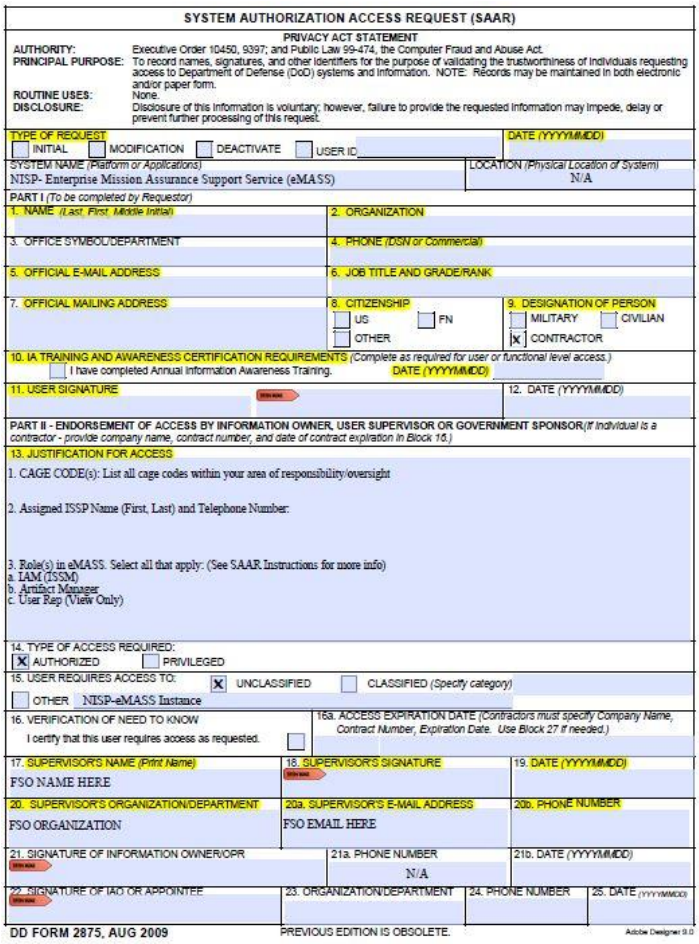
    c. Download the Industry SAAR form and Industry SAAR Instructions.



2. Complete the SAAR in accordance with the Industry SAAR instructions.

   a. All highlighted fields of the SAAR must be completed.

   b. The Facility Security Officer (FSO) or a Key Management Personnel (KMP) member from the CAGE Code(s) identified in Block 13 must complete Blocks 17-20b. This information is validated via the NISS. If needed, the SAAR (Box 27) has space for additional signatures.



SYSTEM AUTHORIZATION ACCESS REQUEST (SAAR)

PRIVACY ACT STATEMENT

AUTHORITY: Executive Order 10450, 9397; and Public Law 99-474, the Computer Fraud and Abuse Act.
PRINCIPAL PURPOSE: To record names, signatures, and other identifiers for the purpose of validating the trustworthiness of individuals requesting access to Department of Defense (DoD) systems and information. NOTE: Records may be maintained in both electronic and/or paper form.
ROUTINE USES: None.
DISCLOSURE: Disclosure of this information is voluntary; however, failure to provide the requested information may impede, delay or prevent further processing of this request.

TYPE OF REQUEST: ☐ INITIAL ☐ MODIFICATION ☐ DEACTIVATE ☐ USER ID
DATE (YYYYMMDD)

SYSTEM NAME (Platform or Applications): NISP- Enterprise Mission Assurance Support Service (eMASS)
LOCATION (Physical Location of System): N/A

PART I (To be completed by Requestor)

1. NAME (Last, First, Middle Initial)
2. ORGANIZATION
3. OFFICE SYMBOL/DEPARTMENT
4. PHONE (DSN or Commercial)
5. OFFICIAL E-MAIL ADDRESS
6. JOB TITLE AND GRADE/RANK
7. OFFICIAL MAILING ADDRESS
8. CITIZENSHIP: ☐ US ☐ FN ☐ OTHER
9. DESIGNATION OF PERSON: ☐ MILITARY ☐ CIVILIAN ☒ CONTRACTOR
10. IA TRAINING AND AWARENESS CERTIFICATION REQUIREMENTS (Complete as required for user or functional level access.) ☐ I have completed Annual Information Awareness Training. DATE (YYYYMMDD)
11. USER SIGNATURE
12. DATE (YYYYMMDD)

PART II - ENDORSEMENT OF ACCESS BY INFORMATION OWNER, USER SUPERVISOR OR GOVERNMENT SPONSOR (If individual is a contractor - provide company name, contract number, and date of contract expiration in Block 16.)

13. JUSTIFICATION FOR ACCESS

1. CAGE CODE(s): List all cage codes within your area of responsibility/oversight

2. Assigned ISSP Name (First, Last) and Telephone Number:

3. Role(s) in eMASS. Select all that apply: (See SAAR Instructions for more info)
a. IAM (ISSM)
b. Artifact Manager
c. User Rep (View Only)

14. TYPE OF ACCESS REQUIRED: ☒ AUTHORIZED ☐ PRIVILEGED
15. USER REQUIRES ACCESS TO: ☒ UNCLASSIFIED ☐ CLASSIFIED (Specify category) ☐ OTHER NISP-eMASS Instance
16. VERIFICATION OF NEED TO KNOW: I certify that this user requires access as requested. ☐
16a. ACCESS EXPIRATION DATE (Contractors must specify Company Name, Contract Number, Expiration Date. Use Block 27 if needed.)
17. SUPERVISOR'S NAME (Print Name): FSO NAME HERE
18. SUPERVISOR'S SIGNATURE
19. DATE (YYYYMMDD)
20. SUPERVISOR'S ORGANIZATION/DEPARTMENT: FSO ORGANIZATION
20a. SUPERVISOR'S E-MAIL ADDRESS: FSO EMAIL HERE
20b. PHONE NUMBER
21. SIGNATURE OF INFORMATION OWNER/OPR
21a. PHONE NUMBER: N/A
21b. DATE (YYYYMMDD)
22. SIGNATURE OF IAO OR APPOINTEE
23. ORGANIZATION/DEPARTMENT
24. PHONE NUMBER
25. DATE (YYYYMMDD)

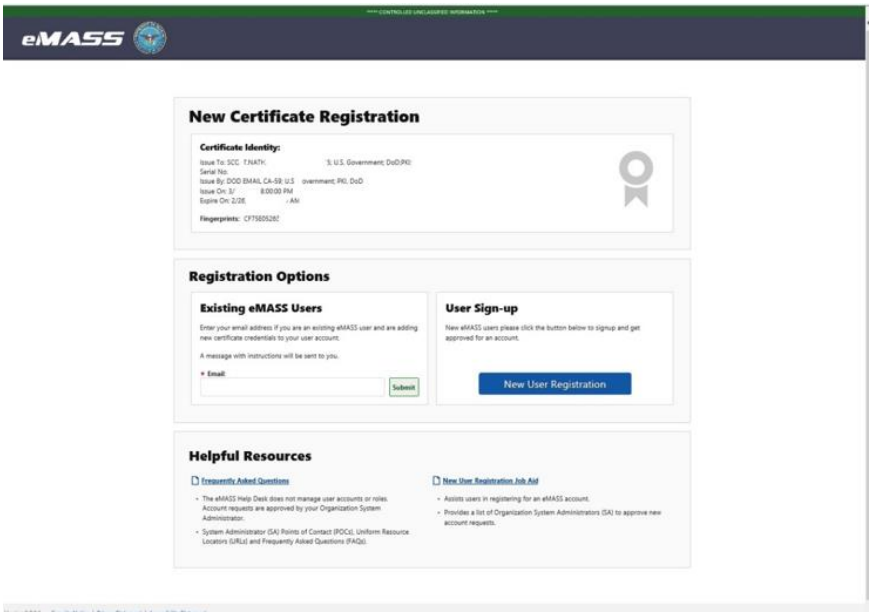
DD FORM 2875, AUG 2009 PREVIOUS EDITION IS OBSOLETE. Adobe Designer 9.0

4 NISP EMASS USER REGISTRATION

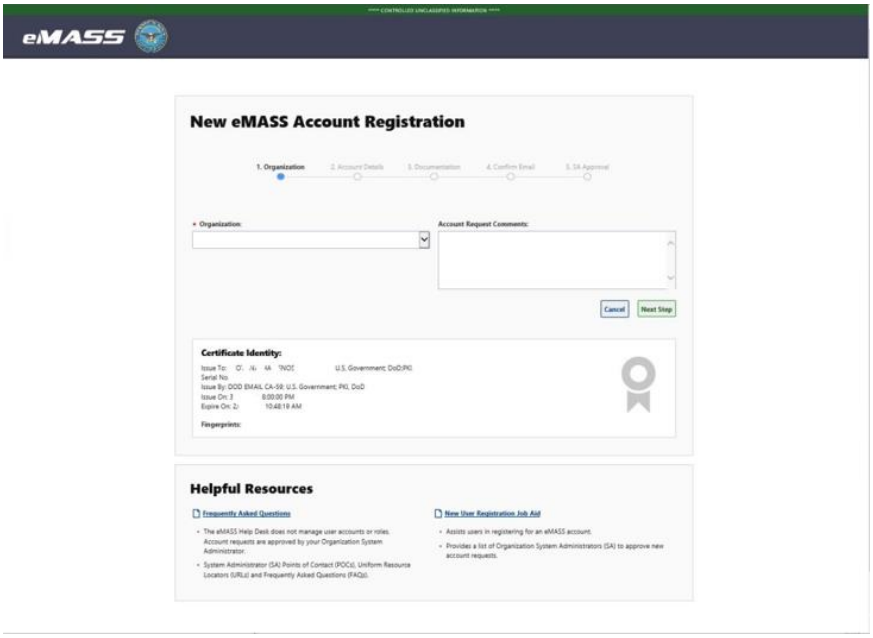
After the training prerequisites and SAAR are completed, Industry will need to complete the following to register their NISP eMASS account:

1. Access the NISP eMASS instance: https://nisp.emass.apps.mil. The eMASS Site Agreement screen is displayed upon PKI authentication. The eMASS Site Agreement message provides the user a warning message that they are accessing a U.S. Government (USG) Information System (IS). Click [Access eMASS] to acknowledge the statement and to access eMASS.

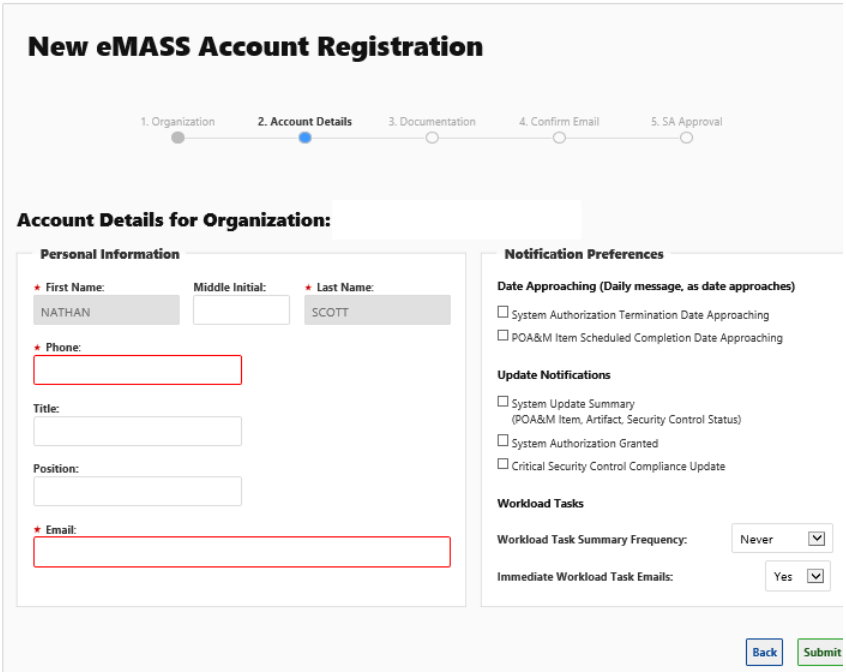
2. Select New User Registration.



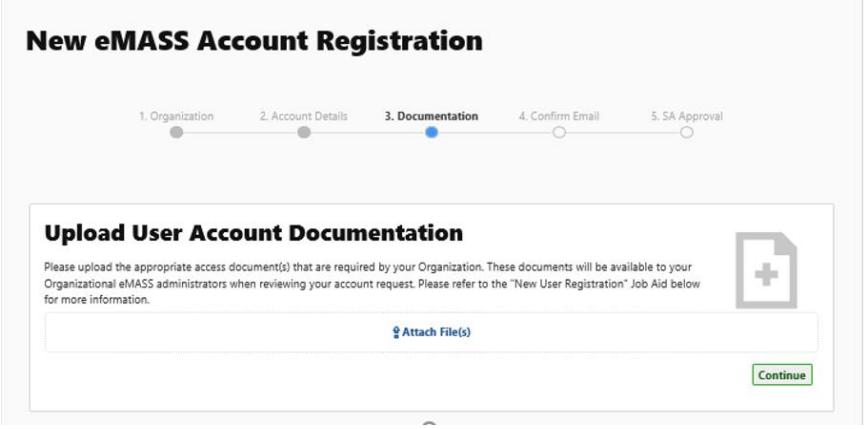
3. Select Organization and provide comments. Industry users must search for their CAGE Code under the Organization dropdown menu. If the CAGE Code is not available, please contact the DCSA NISP Authorization Office (NAO) eMASS Mailbox at dcsa.quantico.dcsa.mbx.emass@mail.mil. Click [Next Step].



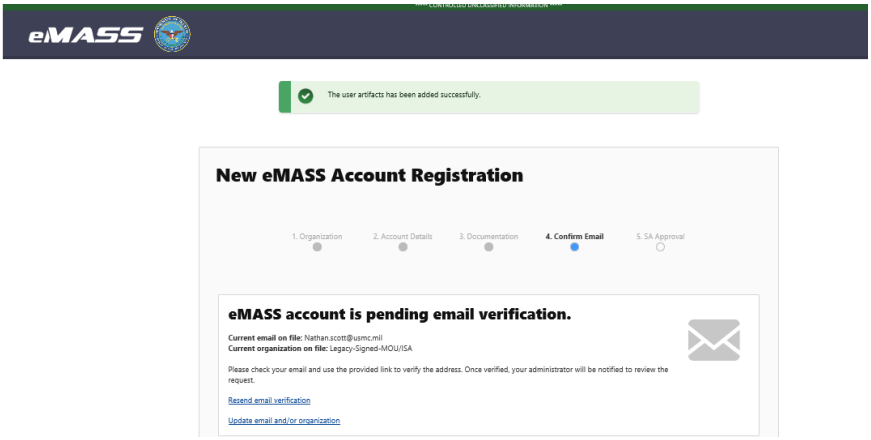
4. Industry must complete all required fields (identified with a red asterisk) in the Account Details step. Notification Preferences allows users to customize their notifications and workload tasks. Once complete, click [Submit].



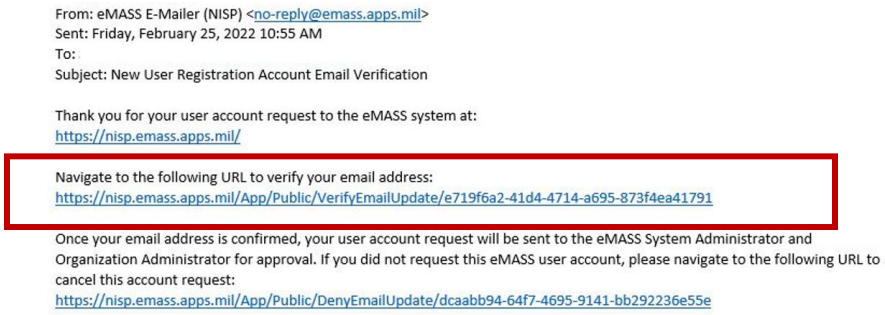
5. In the Documentation step, Industry will upload all the NISP eMASS user account documentation (i.e., eMASS CBT Certificate of Completion, Cyber Awareness Challenge Certificate of Completion, and SAAR). Once complete, click [Continue]. *Note: If the user is unable to successfully upload all user account documentation, submit artifacts to the DCSA NAO mailbox: dcsa.quantico.dcsa.mbx.emass@mail.mil.*



6. A confirmation message will appear stating that the user artifacts have been added successfully. In addition, eMASS will send a verification link to the email address entered during registration. While pending verification, the user has the optional ability to resend the verification email as well as adjust the entered email address and/or selected Home Organization.



7. Upon receiving the automatically generated verification email, the user must click the verification link embedded within the email body in order to verify the pending account request. After verification by the user, the NISP eMASS System Administrators will be able to process and approve the account request.



From: eMASS E-Mailer (NISP) <no-reply@emass.apps.mil>
Sent: Friday, February 25, 2022 10:55 AM
To:
Subject: New User Registration Account Email Verification

Thank you for your user account request to the eMASS system at:
https://nisp.emass.apps.mil/

Navigate to the following URL to verify your email address:
https://nisp.emass.apps.mil/App/Public/VerifyEmailUpdate/e719f6a2-41d4-4714-a695-873f4ea41791

Once your email address is confirmed, your user account request will be sent to the eMASS System Administrator and Organization Administrator for approval. If you did not request this eMASS user account, please navigate to the following URL to cancel this account request:
https://nisp.emass.apps.mil/App/Public/DenyEmailUpdate/dcaabb94-64f7-4695-9141-bb292236e55e

8. The user will receive an email notification when the account has been approved.

For additional information, please contact the assigned ISSP and/or the DCSA NAO eMASS Team at dcsa.quantico.dcsa.mbx.emass@mail.mil.