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 2.0

13 February 2023

TABLE OF CONTENTS

1 INTRODUCTION 1
1.1 BACKGROUND 1
1.2 REQUIREMENTS 1
2 TRAINING PREREQUISITES 2
2.1 EMASS COMPUTER BASED TRAINING 2
2.2 CYBER AWARENESS CHALLENGE TRAINING 3
3 SYSTEM AUTHORIZATION ACCESS REQUEST 5
4 NISP EMASS USER REGISTRATION 11
5 NISP EMASS SYSTEM ASSIGNMENT 14

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 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 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 user 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).

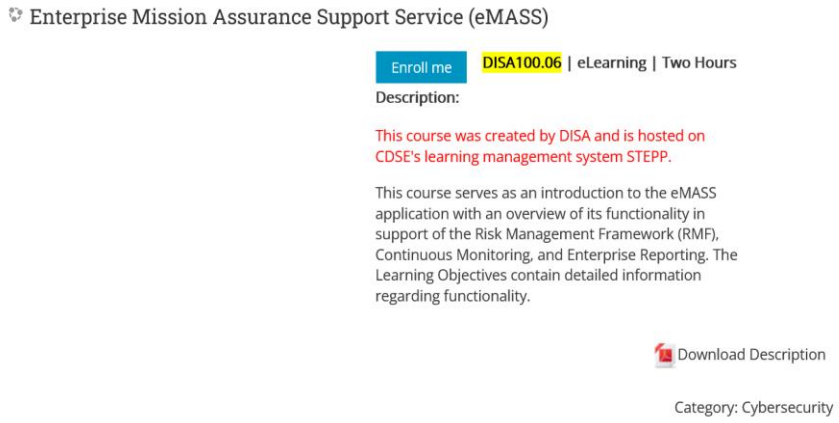
Cleared Industry users requiring access to the NISP eMASS instance must also have a Department of Defense (DoD) Public Key Infrastructure (PKI) certificate on an External Certification Authority (ECA) or Common Access Card (CAC). Cleared Industry contractors should only use issued DoD credentials associated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

2 TRAINING PREREQUISITES

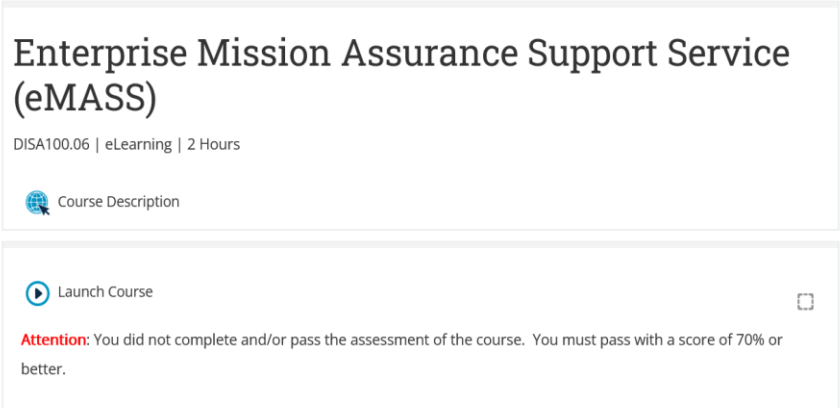
2.1 EMASS COMPUTER BASED TRAINING

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 Center for Development of Security Excellence (CDSE) Security Training, Education, and Professionalization Portal (STEPP). Industry will perform the following actions:

1. Access the CDSE STEPP site: https://cdse.usalearning.gov/login/index.php
2. Accept the DoD Acceptable Use Policy.
3. Login with existing credentials (i.e., username and password) or create new account.
4. Search for Course DISA100.06 (Enterprise Mission Assurance Support Service (eMASS)).



5. Launch and complete the eMASS CBT. The eMASS CBT takes approximately 2 hours to complete and must be completed in one session.



6. 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 Training certificate completion dates cannot be greater than one year of the account request.*

For questions related to the STEPP site, passwords, account navigation, course offerings, or eLearning courses, see the list of FAQs located on the right hand side of the site. If you do not see an answer to your question, please contact the STEPP Help Desk at 202-753-0845.

eMASS CBT questions should be directed to the DISA eMASS Tier III Helpdesk: disa.meade.id.mbx.emass-tier-iii-support@mail.mil

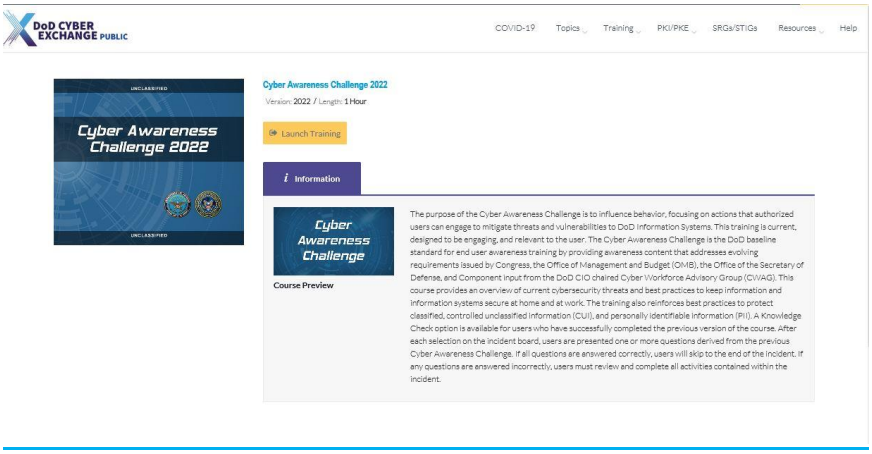
2.2 CYBER AWARENESS CHALLENGE TRAINING

Industry users must complete the Cyber Awareness Challenge training prior to being granted access to the NISP eMASS. The training is available on both the CDSE STEPP and DoD Cyber Exchange sites. In order to complete the training, Industry will perform the following actions on the selected site:

DoD Cyber Exchange Public Site

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

2. Select "Launch Training".



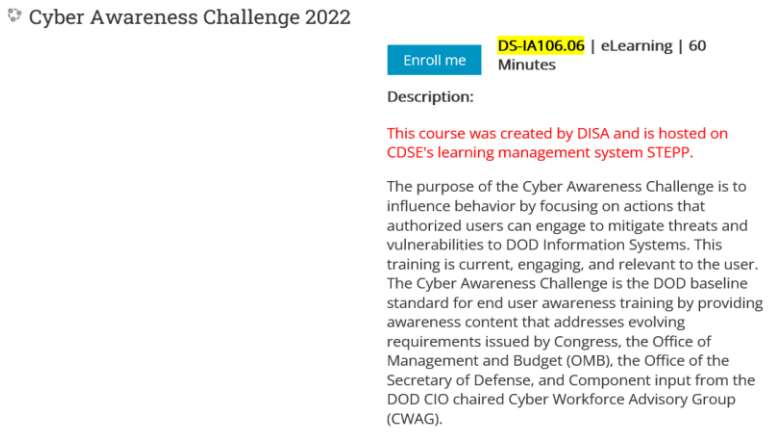
3. Select "Start New Session".

4. After completing the training, save a copy of the certificate of completion. *Note: 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/.

CDSE STEPP Site

1. Access the CDSE STEPP site: https://cdse.usalearning.gov/login/index.php
2. Accept the DoD Acceptable Use Policy.
3. Login with existing credentials (i.e., username and password) or create new account.
4. Search for Course DS-IA106.06 (Cyber Awareness Challenge).



5. Launch and complete the Cyber Awareness Challenge.
6. 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 Training certificate completion dates cannot be greater than one year of the account request.*

For questions related to the STEPP site, passwords, account navigation, course offerings, or eLearning courses, see the list of FAQs located on the right hand side of the site. If you do not see an answer to your question, please contact the STEPP Help Desk at 202-753-0845.

3 SYSTEM AUTHORIZATION ACCESS REQUEST

Industry users must complete and submit the Industry System Authorization Access Request (SAAR) (DD Form 2875, May 2022) prior to being granted access to the NISP eMASS. Industry will perform the following actions:

1. Obtain the Industry SAAR form at the DCSA site: https://www.dcsa.mil/

2. Within the top portion of the SAAR, the requestor will select the classification level (UNCLASSIFIED), Type of Request, and enter the date (YYYYMMDD). The remaining fields (User ID, System Name, and Location) should align with the guidance and example provided below:

   TYPE OF REQUEST: Use the drop-down menu to select the applicable request type.

   a. INTIAL: Selected for initial NISP eMASS user account requests. "Initial" is also selected when a current NISP eMASS user account needs to be reactivated after over 90 days of inactivity.

   b. MODIFICATION: Selected when an additional NISP eMASS role and/or CAGE Code access is requested for a current NISP eMASS user account.

   c. DEACTIVATE: Selected when the employment status of an employee changes (i.e., termination, retirement, etc.) and the NISP eMASS user account must be deactivated. **IMPORTANT** If the employment status of an employee changes (i.e., termination, retirement, etc.), the FSO and/or member of the KMP is responsible for requesting deactivation of the user's account by submitting a DCSA SAAR to the DCSA NISP Authorization Office (NAO) eMASS Team at dcsa.quantico.dcsa.mbx.emass@mail.mil.

   USER ID: Leave blank.

   DATE: Enter date (YYYYMMDD) of the request.

   SYSTEM NAME: Ensure "NISP Enterprise Mission Assurance Support Service" is entered.

   LOCATION: Enter "Not Applicable".

UNCLASSIFIED

SYSTEM AUTHORIZATION ACCESS REQUEST (SAAR)

OMB No. 0704-0630
OMB approval expires: 20260631

The public reporting burden for this collection of information, 0704-0630, is estimated to average 5 minutes per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding the burden estimate or burden reduction suggestions to the Department of Defense, Washington Headquarters Services, at whs.mc-alex.esd.mbx.dd-dod-information-collections@mail.mil. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to any penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.

PRIVACY ACT STATEMENT

AUTHORITY: Executive Order 10450; and Public Law 99-474, the Computer Fraud and Abuse Act
PRINCIPAL PURPOSE(S): 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 USE(S): 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	USER ID	DATE (YYYYMMDD)
INITIAL	LEAVE BLANK	20221229

SYSTEM NAME (Platform or Applications)	LOCATION (Physical Location of System)
NISP Enterprise Mission Assurance Support Service	NOT APPLICABLE

INDUSTRY SAAR – PART I

3. Within Part I of the SAAR, the requestor will enter their administrative data.

BLOCK 1 – NAME: Enter Last, First, and Middle Initial.

BLOCK 2 – ORGANIZATION: Enter Company/Facility Name.

BLOCK 3 – OFFICE SYMBOL/DEPARTMENT: Enter office symbol/department within the company. If not applicable, leave blank.

BLOCK 4 – PHONE: Enter phone number.

BLOCK 5 – OFFICIAL E-MAIL ADDRESS: Enter official email address. This email address must align with the email address entered during NISP eMASS user registration (See Section 4 – NISP eMASS User Registration).

BLOCK 6 – JOB TITLE AND GRADE/RANK: Enter official job title (e.g., Information Systems Security Manager, Information Systems Security Officer, Facility Security Officer, etc.).

BLOCK 7 – OFFICIAL MAILING ADDRESS: Enter the mailing address of the company/facility.

BLOCK 8 – CITIZENSHIP: Mark the applicable citizenship status (i.e., US).

BLOCK 9 – DESIGNATION OF PERSON: Mark the applicable designation (i.e., Contractor).

BLOCK 10 – IA TRAINING AND AWARENESS CERTIFICATION REQUIREMENTS: The requestor must indicate if they have completed the Annual Information Awareness Training (i.e., Cyber Awareness Challenge) and provide the date (YYYYMMDD) of completion.

BLOCK 11 – USER SIGNATURE: The requestor must sign the Industry SAAR. By signing, the requestor is certifying that a NISP eMASS user account is required to perform system security program responsibilities. In addition, the requestor is attesting that all information is true and correct.

BLOCK 12 – DATE: Enter the date (YYYYMMDD) that Block 11 was signed by the requestor.

<table>
<tr><td colspan="3">PART I (To be completed by Requester)</td></tr>
<tr><td>1. NAME (Last, First, Middle Initial)
DOE, JOHN</td><td colspan="2">2. ORGANIZATION
COMPANY ABC</td></tr>
<tr><td>3. OFFICE SYMBOL/DEPARTMENT
SECURITY OFFICE</td><td colspan="2">4. PHONE (DSN or Commercial)
555-555-5555</td></tr>
<tr><td>5. OFFICIAL E-MAIL ADDRESS
JOHN.DOE@ABC.COM</td><td colspan="2">6. JOB TITLE AND GRADE/RANK
INFORMATION SYSTEMS SECURITY MANAGER</td></tr>
<tr><td>7. OFFICIAL MAILING ADDRESS
123 EMASS LANE
BOSTON, MA 02108</td><td>8. CITIZENSHIP
☒ US ☐ FN
☐ OTHER</td><td>9. DESIGNATION OF PERSON
☐ MILITARY ☐ CIVILIAN
☒ CONTRACTOR</td></tr>
<tr><td colspan="3">10. IA TRAINING AND AWARENESS CERTIFICATION REQUIREMENTS (Complete as required for user or functional level access.)
☒ I have completed the Annual Cyber Awareness Training. DATE (YYYYMMDD) 20221201</td></tr>
<tr><td colspan="2">11. USER SIGNATURE
SIGNATURE OF REQUESTOR</td><td>12. DATE (YYYYMMDD)
20221229</td></tr>
</table>

INDUSTRY SAAR – PART II

4. Within Part II of the SAAR, the justification for access and endorsement will be completed.

BLOCK 13 – JUSTIFICATION FOR ACCESS: Within this block, the requestor will identify the CAGE Code(s), assigned Information Systems Security Professional (ISSP), and requested NISP eMASS roles. **IMPORTANT** All this information must be entered in order to process a NISP eMASS request. If this information is not complete, the request will be denied.

a. CAGE CODE(s): List CAGE Code(s) within your area of responsibility/oversight. The CAGE Code must have a FCL and approved safeguarding.

b. ASSIGNED ISSP NAME (First, Last): Provide the name of the assigned DCSA ISSP.

c. REQUESTED ROLE(S): Identify the requested role(s). The following are the available Industry NISP eMASS roles: (1) Information Assurance Manager (IAM), (2) Artifact Manager, (3) View Only and (4) Ad Hoc. Below is a description of each role.

- Information Assurance Manager (IAM): This role is intended for users that will be directly responsible for performing system security program responsibilities and conducting the testing of systems' compliance with the RMF security requirements. Permissions include the following: registering system records, populating system details, editing security controls, submitting security controls, initiating and submitting workflows, uploading artifacts, and conducting system roles assignments.

- Artifact Manager: This role is intended for users that will have a limited responsibility for activities within eMASS but require visibility into the system record. Artifact Managers have view-only permissions but can also create, edit, and delete artifacts related to an assigned system record.

- View Only: This role is intended for users that will not be responsible for activities within eMASS but require visibility into the system record. Users with this role will have view-only permissions.

- Ad Hoc: This role is intended for users that require full access to Executive Reports for their assigned CAGE Code(s). NISP eMASS users with traditional user roles (e.g., IAM) will have default access to Executive Reports, but the dashboard results will only display assigned systems (rather than all systems within a CAGE Code).***IMPORTANT** When users are assigned to all systems under their CAGE Code(s), they will have access to run Executive Reports for all systems. This role will only be selected if the user will NOT be assigned to all systems. This role alone does not provide permissions to perform system record activities (e.g., registering systems records, populating system details, editing security controls, uploading artifacts, etc.).

BLOCK 14 – TYPE OF ACCESS REQUESTED: Ensure "AUTHORIZED" is marked. *Note: "PRIVILEGED" access is not applicable for Industry users.*

BLOCK 15 – USER REQUIRES ACCESS TO: Ensure "OTHER" is marked and "National Industrial Security Program Enterprise Mission Assurance Support Service" is entered.

BLOCK 16 – VERIFICATION OF NEED TO KNOW: The individual endorsing the request (Blocks 17-17e) will mark this section in order to verify that the user requires access as requested.

BLOCK 16a – ACCESS EXPIRATION DATE: Enter "Not Applicable".

BLOCK 17 – SUPERVISOR'S NAME: Enter the first and last name of the FSO and/or member of the KMP from the CAGE Code identified in Block 13. This information is validated via the NISS.

BLOCK 17a – SUPERVISOR'S EMAIL ADDRESS: Enter the official email address of the FSO and/or member of the KMP.

BLOCK 17b – SUPERVISOR'S PHONE NUMBER: Enter phone number of the FSO and/or member of the KMP.

BLOCK 17c – SUPERVISOR'S ORGANIZATION/DEPARTMENT: Enter the Organization/Department of the FSO and/or member of the KMP.

BLOCK 17d – SUPERVISOR'S SIGNATURE: The FSO and/or member of the KMP will endorse the request by signing here. By signing, the FSO and/or KMP is stating that the requestor is able to have a NISP eMASS user account and perform system security program responsibilities.

BLOCK 17e – DATE: Enter the date (YYYYMMDD) that Block 17d was signed by the FSO and/or member of the KMP.

BLOCKS 18 – 19c: Leave blank.

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) : 12345 2. ASSIGNED ISSP : ISSP JANE SMITH 3. REQUESTED ROLE(S): IAM		
14. TYPE OF ACCESS REQUESTED ☒ AUTHORIZED ☐ PRIVILEGED		
15. USER REQUIRES ACCESS TO: ☐ UNCLASSIFIED ☐ CLASSIFIED *(Specify category)* ☒ OTHER NATIONAL INDUSTRIAL SECURITY PROGRAM ENTERPRISE MISSION ASSURANCE SUPPORT SERVICE		
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 21 if needed.)* NOT APPLICABLE	
17. SUPERVISOR'S NAME *(Print Name)* FSO - JOE BLOGGS	**17a. SUPERVISOR'S EMAIL ADDRESS** JOE.BLOGGS@ABC.COM	**17b. PHONE NUMBER** 555-555-5555
17c. SUPERVISOR'S ORGANIZATION/DEPARTMENT ABC SECURITY OFFICE	**17d. SUPERVISOR SIGNATURE** *SIGNATURE OF FSO AND/OR KMP*	**17e. DATE** *(YYYYMMDD)* 20221229
18. INFORMATION OWNER/OPR PHONE NUMBER LEAVE BLANK	**18a. INFORMATION OWNER/OPR SIGNATURE**	**18b. DATE** *(YYYYMMDD)*
19. ISSO ORGANIZATION/DEPARTMENT LEAVE BLANK **19a. PHONE NUMBER**	**19b. ISSO OR APPOINTEE SIGNATURE**	**19c. DATE** *(YYYYMMDD)*

BLOCK 21 – OPTIONAL INFORMATION: If more than one CAGE Code is listed in Block 13, this section can be used to enter additional FSO and/or member of the KMP information.
IMPORTANT The FSO and/or member of the KMP from EACH CAGE Code listed in Block 13 is required to endorse/sign the SAAR. The additional signature blocks (18a and 19b) can be used. The requestor can also submit a separate SAAR for each CAGE Code.

INDUSTRY SAAR – PART III AND PART IV

5. Part III and Part IV of the SAAR are not required. Leave these sections blank.

INDUSTRY SAAR EXAMPLE

UNCLASSIFIED

SYSTEM AUTHORIZATION ACCESS REQUEST (SAAR)

OMB No. 0704-0630
OMB approval expires: 20250631

PRIVACY ACT STATEMENT

AUTHORITY: Executive Order 10450; and Public Law 99-474, the Computer Fraud and Abuse Act
PRINCIPAL PURPOSE(S): 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 USE(S): 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	USER ID	DATE (YYYYMMDD)
INITIAL	LEAVE BLANK	20221229

SYSTEM NAME (Platform or Applications)	LOCATION (Physical Location of System)
NISP Enterprise Mission Assurance Support Service	NOT APPLICABLE

PART I *(To be completed by Requester)*

1. NAME (Last, First, Middle Initial)	2. ORGANIZATION
DOE, JOHN	COMPANY ABC
3. OFFICE SYMBOL/DEPARTMENT	**4. PHONE (DSN or Commercial)**
SECURITY OFFICE	555-555-5555
5. OFFICIAL E-MAIL ADDRESS	**6. JOB TITLE AND GRADE/RANK**
JOHN.DOE@ABC.COM	INFORMATION SYSTEMS SECURITY MANAGER

7. OFFICIAL MAILING ADDRESS
123 EMASS LANE
BOSTON, MA 02108

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 the Annual Cyber Awareness Training. DATE (YYYYMMDD) 20221201

11. USER SIGNATURE	12. DATE (YYYYMMDD)
SIGNATURE OF REQUESTOR	20221229

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) : 12345
2. ASSIGNED ISSP : ISSP JANE SMITH
3. REQUESTED ROLE(S): IAM

14. TYPE OF ACCESS REQUESTED
☒ AUTHORIZED ☐ PRIVILEGED

15. USER REQUIRES ACCESS TO: ☐ UNCLASSIFIED ☐ CLASSIFIED *(Specify category)*
☒ OTHER NATIONAL INDUSTRIAL SECURITY PROGRAM ENTERPRISE MISSION ASSURANCE SUPPORT SERVICE

16. VERIFICATION OF NEED TO KNOW	16a. ACCESS EXPIRATION DATE *(Contractors must specify Company Name, Contract Number, Expiration Date. Use Block 21 if needed.)*	
☒ I certify that this user requires access as requested.	NOT APPLICABLE	
17. SUPERVISOR'S NAME *(Print Name)*	**17a. SUPERVISOR'S EMAIL ADDRESS**	**17b. PHONE NUMBER**
FSO - JOE BLOGGS	JOE.BLOGGS@ABC.COM	555-555-5555
17c. SUPERVISOR'S ORGANIZATION/DEPARTMENT	**17d. SUPERVISOR SIGNATURE**	**17e. DATE (YYYYMMDD)**
ABC SECURITY OFFICE	SIGNATURE OF FSO AND/OR KMP	20221229
18. INFORMATION OWNER/OPR PHONE NUMBER	**18a. INFORMATION OWNER/OPR SIGNATURE**	**18b. DATE (YYYYMMDD)**
LEAVE BLANK		
19. ISSO ORGANIZATION/DEPARTMENT	**19b. ISSO OR APPOINTEE SIGNATURE**	**19c. DATE (YYYYMMDD)**
LEAVE BLANK		
19a. PHONE NUMBER		

DD FORM 2875, MAY 2022 UNCLASSIFIED Page 1 of 3

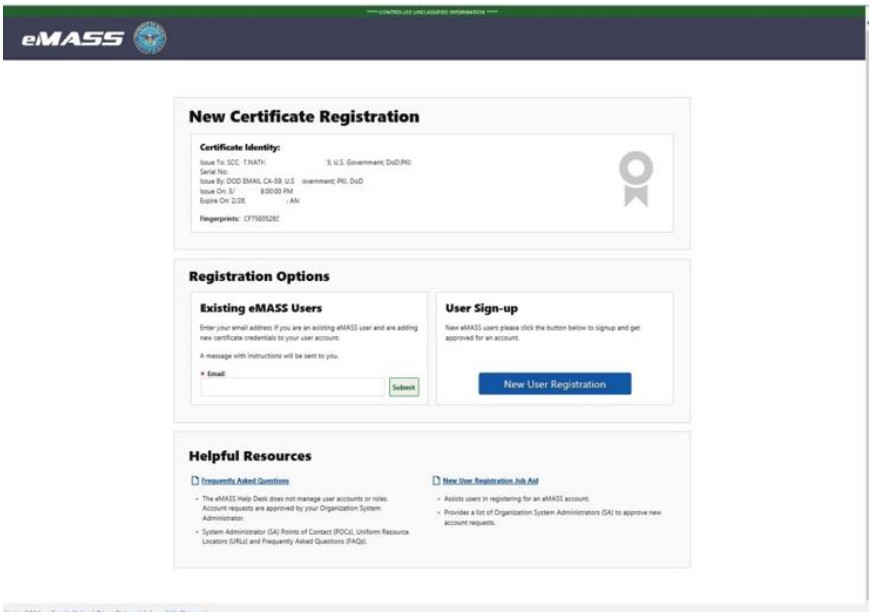
PREVIOUS EDITION IS OBSOLETE.

4 NISP EMASS USER REGISTRATION

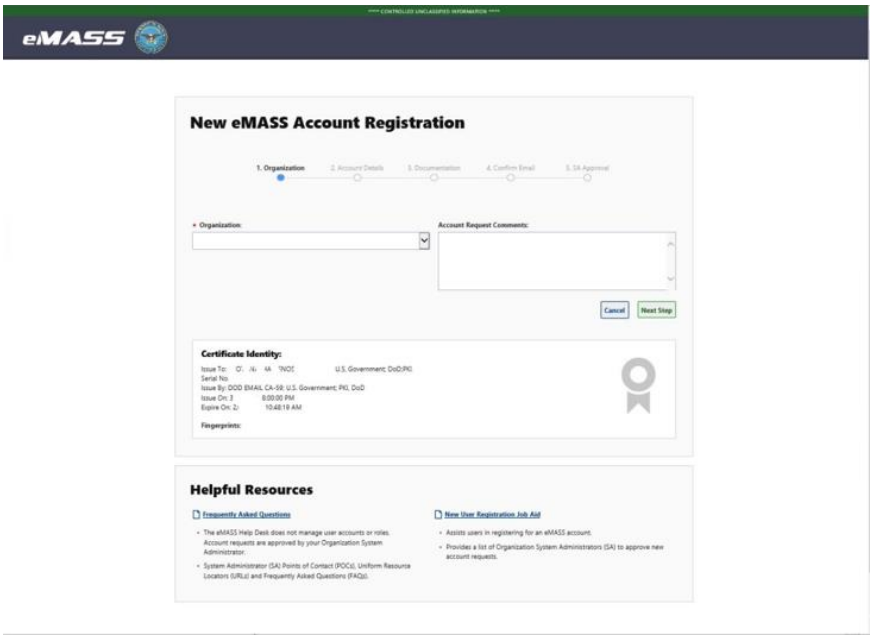
After the training prerequisites and SAAR are completed, Industry will need to complete the following to register their NISP eMASS user account:

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.

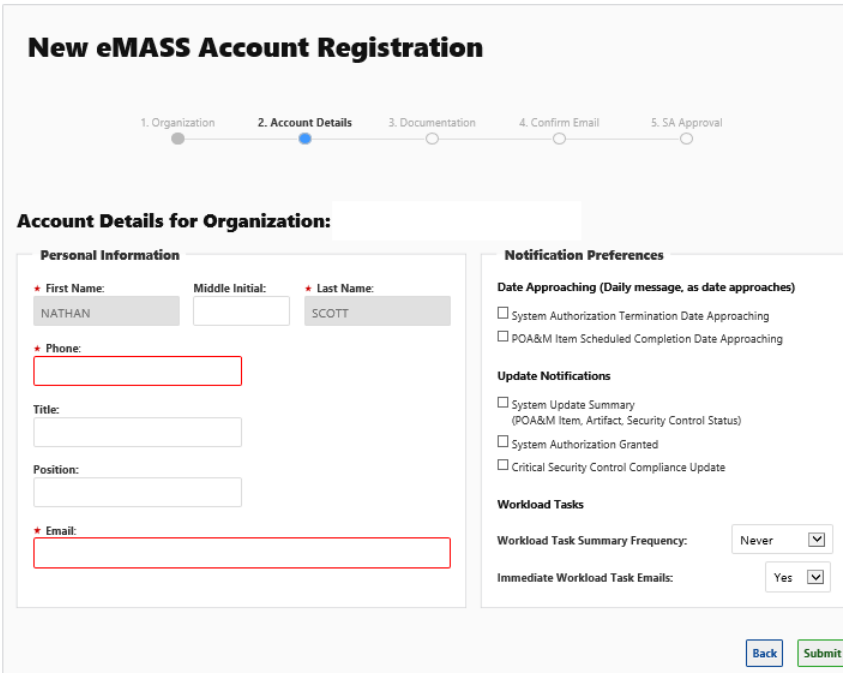
2. Select New User Registration.



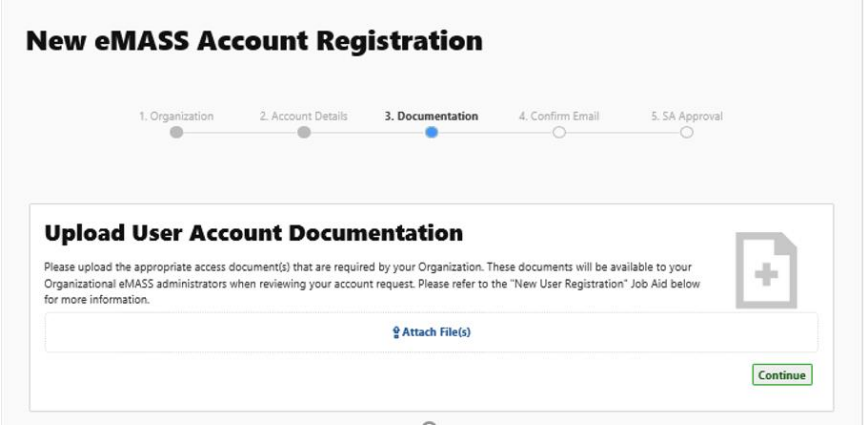
3. Select Organization and provide comments. Industry users must search for their CAGE Code under the Organization dropdown menu. Click [Next Step]. *Note: If the CAGE Code is not available, please contact the DCSA NAO eMASS Team at dcsa.quantico.dcsa.mbx.emass@mail.mil.*



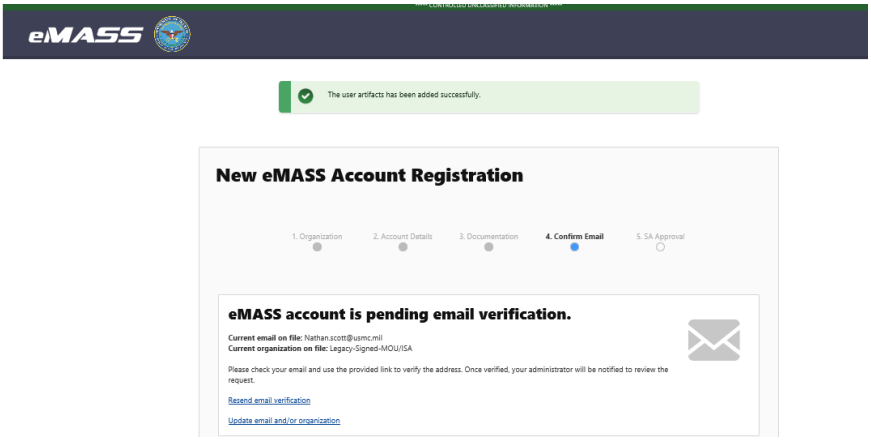
4. Industry must complete all required fields (identified with a red asterisk) in the Account Details step. Notification Preferences allows users to customize their notifications and workload tasks. Once complete, click [Submit].



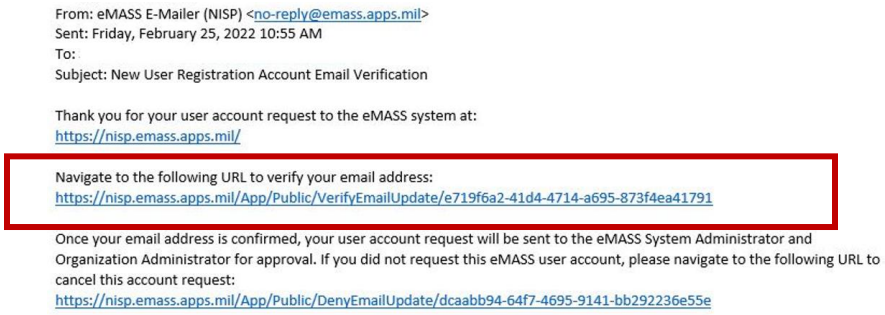
5. In the Documentation step, Industry will upload all the NISP eMASS user account documentation (i.e., eMASS CBT Certificate of Completion, Cyber Awareness Challenge Certificate of Completion, and SAAR). Once complete, click [Continue]. *Note: If the user is unable to successfully upload all user account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

5 NISP EMASS SYSTEM ASSIGNMENT

Once a NISP eMASS user account request is approved, the user will not have immediate access to the system(s) under their associated CAGE Code(s). The NISP eMASS user account approval process involves approving role and CAGE Code access. The DCSA NAO eMASS Team (NISP eMASS System Administrators) does not assign users to systems. Users are initially assigned to systems during "New System Registration". For systems already registered within a CAGE Code, an IAM assigned to the system is responsible for assigning additional users. An IAM assigned to the system will conduct the following actions:

1. Select the system;

2. Within the Management module, select Personnel;

3. Click Edit in the applicable approval chains (i.e., Control Approval Chain and Package Approval Chain); and

4. Within the specific role, drag the user's name from the Available Users list box to the Assigned Users list box or double-click on the user's name in the Available Users list box.

When conducting role assignment via Management > Personnel within a system, the available users within the Industry roles (e.g., IAM, Artifact Manager, View Only) will be the NISP eMASS users that have an active NISP eMASS user account that includes the applicable role and CAGE Code access.

Note: If an IAM is not assigned to active system(s) under a CAGE Code, please contact the DCSA NAO eMASS Team (dcsa.quantico.dcsa.mbx.emass@mail.mil) for system assignment.