

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 1.1

06 May 2022



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	7



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 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)).

Enterprise Mission Assurance Support Service (eMASS)

Enroll me **DISA100.06** | eLearning | Two Hours

Description:

This course was created by DISA and is hosted on CDSE's learning management system STEPP.

This course serves as an introduction to the eMASS application with an overview of its functionality in support of the Risk Management Framework (RMF), Continuous Monitoring, and Enterprise Reporting. The Learning Objectives contain detailed information regarding functionality.


 Download Description



Category: Cybersecurity

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

Enterprise Mission Assurance Support Service (eMASS)

DISA100.06 | eLearning | 2 Hours

 Course Description

 Launch Course 

Attention: You did not complete and/or pass the assessment of the course. You must pass with a score of 70% or better.



- 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 Help Desk at 202-753-0845.

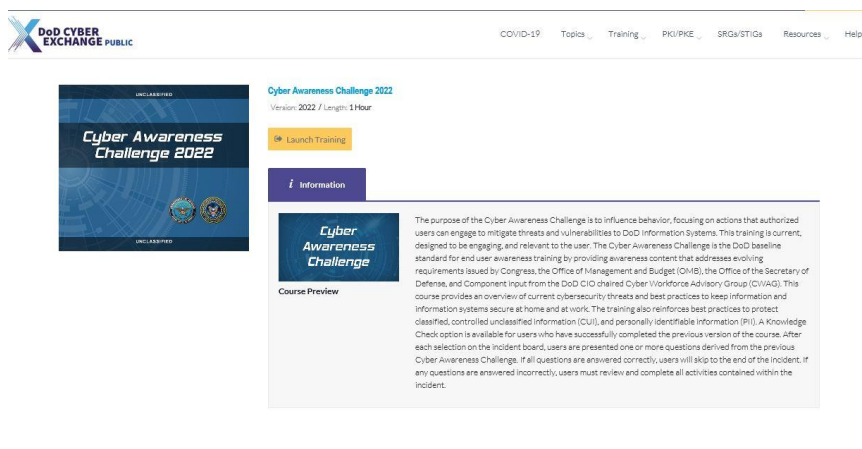
eMASS CBT questions should be directed to the DISA eMASS Tier III Helpdesk: disa.meade.id.mbx.emass-tier-iii-support@mail.mil

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

- Access the training on the DoD Cyber Exchange Public site:
<https://public.cyber.mil/training/cyber-awareness-challenge/>
- Select “Launch Training”.



- Select “Start New Session”.
- 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).

🔖 Cyber Awareness Challenge 2022

Enroll me

DS-IA106.06 | eLearning | 60
Minutes

Description:

This course was created by DISA and is hosted on CDSE's learning management system STEPP.

The purpose of the Cyber Awareness Challenge is to influence behavior by focusing on actions that authorized users can engage to mitigate threats and vulnerabilities to DOD Information Systems. This training is current, engaging, and relevant to the user. The Cyber Awareness Challenge is the DOD baseline standard for end user awareness training by providing awareness content that addresses evolving requirements issued by Congress, the Office of Management and Budget (OMB), the Office of the Secretary of Defense, and Component input from the DOD CIO chaired Cyber Workforce Advisory Group (CWAG).

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 Help Desk at 202-753-0845.



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/isd/tools/>
 - a. Select the eMASS Tab
 - b. Select Account Management
 - c. Download the Industry SAAR form and Industry SAAR Instructions.

NISP Resources **eMASS** RMF FOCI Contact Us

NISP Enterprise Mission Assurance Support Service (EMASS)

Account Management

To request a NISP eMASS user account, cleared Industry must complete the following:

1. DISA eMASS Computer Based Training (CBT)
2. Cyber Awareness Challenge (CAC) Training
3. DCSA System Authorization Access Request (SAAR) Form
4. NISP eMASS User Registration (<https://nisp.emass.apps.mil>)

In order to ensure successful completion of all the NISP eMASS user account prerequisites, follow the guidance in the NISP eMASS User Account Request Guide. For additional information, please contact the assigned Information Systems Security Professional (ISSP) and/or the DCSA NAO eMASS Team at dcsa.quantico.dcsa.mbx.emass@mail.mil.

- NISP eMASS User Account Request Guide
- **Industry SAAR Instructions**
- **Industry SAAR Form**
- Field Office Facilities



DEFENSE COUNTERINTELLIGENCE AND SECURITY AGENCY

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)			
<p>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.</p>			
TYPE OF REQUEST: <input type="checkbox"/> INITIAL <input type="checkbox"/> MODIFICATION <input type="checkbox"/> DEACTIVATE <input type="checkbox"/> 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: <input type="checkbox"/> US <input type="checkbox"/> FN <input type="checkbox"/> OTHER	
		9. DESIGNATION OF PERSON: <input type="checkbox"/> MILITARY <input type="checkbox"/> CIVILIAN <input checked="" type="checkbox"/> CONTRACTOR	
10. IA TRAINING AND AWARENESS CERTIFICATION REQUIREMENTS (Complete as required for user or functional level access.) <input type="checkbox"/> 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 14.)			
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. Armixt Manager c. User Rep (View Only)			
14. TYPE OF ACCESS REQUIRED: <input checked="" type="checkbox"/> AUTHORIZED <input type="checkbox"/> PRIVILEGED			
15. USER REQUIRES ACCESS TO: <input checked="" type="checkbox"/> UNCLASSIFIED <input type="checkbox"/> CLASSIFIED (Specify category) <input type="checkbox"/> OTHER NISP-eMASS Instance			
16. VERIFICATION OF NEED TO KNOW I certify that this user requires access as requested. <input type="checkbox"/>		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.



eMASS Site Agreement

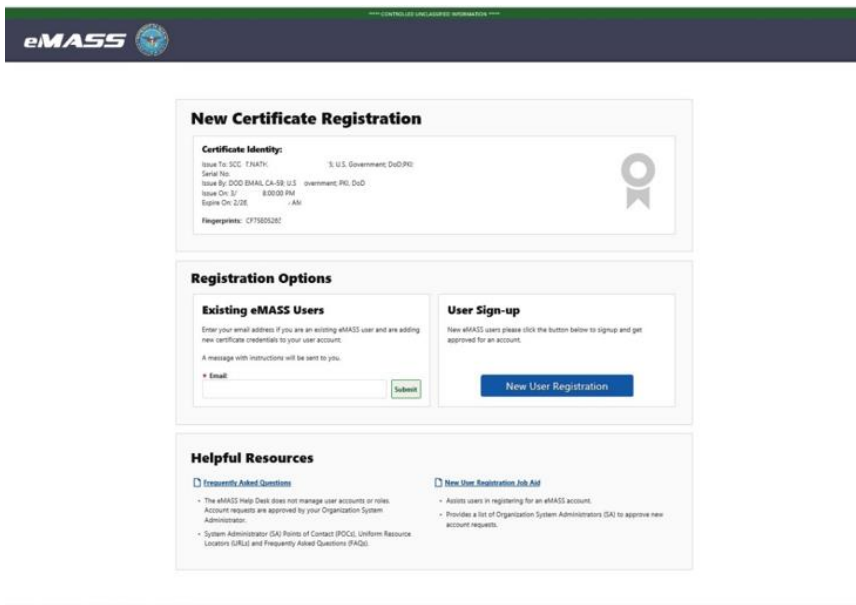
You are accessing a U.S. Government (USG) Information System (IS) that is provided for USG-authorized use only. By using this IS (which includes any device attached to this IS), you consent to the following conditions:

- The USG routinely intercepts and monitors communications on this IS for purposes including, but not limited to, penetration testing, COMSEC monitoring, network operations and defense, personnel misconduct (PM), law enforcement (LE), and counterintelligence (CI) investigations.
- At any time, the USG may inspect and seize data stored on this IS.
- Communications using, or data stored on, this IS are not private, are subject to routine monitoring, interception, and search, and may be disclosed or used for any USG authorized purpose.
- This IS includes security measures (e.g., authentication and access controls) to protect USG interests—not for your personal benefit or privacy.
- Notwithstanding the above, using this IS does not constitute consent to PM, LE or CI investigative searching or monitoring of the content of privileged communications, or work product, related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants. Such communications and work product are private and confidential. See User Agreement for details.



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].



- 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 NISP Authorization Office (NAO) mailbox: dcsa.quantico.dcsa.mbx.emass@mail.mil.*

New eMASS Account Registration

1. Organization 2. Account Details 3. Documentation 4. Confirm Email 5. SA Approval

Upload User Account Documentation

Please upload the appropriate access document(s) that are required by your Organization. These documents will be available to your Organizational eMASS administrators when reviewing your account request. Please refer to the "New User Registration" Job Aid below for more information.

[Attach File\(s\)](#)

[Continue](#)

- 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.

eMASS

The user artifacts has been added successfully.

New eMASS Account Registration

1. Organization 2. Account Details 3. Documentation 4. Confirm Email 5. SA Approval

eMASS account is pending email verification.

Current email on file: Nathan.scott@usmc.mil
Current organization on file: Legacy-Signed-MOU/ISA

Please check your email and use the provided link to verify the address. Once verified, your administrator will be notified to review the request.

[Resend email verification](#)

[Update email and/or 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 additional information, please contact the assigned Information Systems Security Professional (ISSP) and/or the DCSA NAO eMASS Team at dcsa.quantico.dcsa.mbx.emass@mail.mil.