





**TABLE OF CONTENTS**

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















## INDUSTRY SAAR – PART II

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.**

- ☒ CAGE CODE(s): List CAGE Code(s) within your area of responsibility/oversight. The CAGE Code must have an FCL and approved safeguarding.
- ☒ ASSIGNED ISSP NAME (First, Last): Provide the name of the assigned DCSA ISSP.
- ☒ 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. **Note:** *The signature cannot be greater than 30 days old from the account request.*

**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.



# DEFENSE COUNTERINTELLIGENCE AND SECURITY AGENCY

<b>PART II ENDORSEMENT OF ACCESS BY INFORMATION OWNER, USER SUPERVISOR OR GOVERNMENT SPONSOR</b> <i>(If individual is a contractor - provide company name, contract number, and date of contract expiration in Block 16.)</i>		
<b>13. JUSTIFICATION FOR ACCESS</b> 1. CAGE CODE(s) : 12345 2. ASSIGNED ISSP : ISSP JANE SMITH 3. REQUESTED ROLE(S): IAM		
<b>14. TYPE OF ACCESS REQUESTED</b> <input checked="" type="checkbox"/> AUTHORIZED <input type="checkbox"/> PRIVILEGED		
<b>15. USER REQUIRES ACCESS TO:</b> <input type="checkbox"/> UNCLASSIFIED <input type="checkbox"/> CLASSIFIED <i>(Specify category)</i> <input checked="" type="checkbox"/> OTHER NATIONAL INDUSTRIAL SECURITY PROGRAM ENTERPRISE MISSION ASSURANCE SUPPORT SERVICE		
<b>16. VERIFICATION OF NEED TO KNOW</b> <input checked="" type="checkbox"/> I certify that this user requires access as requested.	<b>16a. ACCESS EXPIRATION DATE</b> <i>(Contractors must specify Company Name, Contract Number, Expiration Date. Use Block 21 if needed.)</i> NOT APPLICABLE	
<b>17. SUPERVISOR'S NAME</b> <i>(Print Name)</i> FSO - JOE BLOGGS	<b>17a. SUPERVISOR'S EMAIL ADDRESS</b> JOE.BLOGGS@ABC.COM	<b>17b. PHONE NUMBER</b> 555-555-5555
<b>17c. SUPERVISOR'S ORGANIZATION/DEPARTMENT</b> ABC SECURITY OFFICE	<b>17d. SUPERVISOR SIGNATURE</b>  SIGNATURE OF FSO AND/OR KMP	<b>17e. DATE</b> <i>(YYYYMMDD)</i> 20221229
<b>18. INFORMATION OWNER/OPR PHONE NUMBER</b> LEAVE BLANK	<b>18a. INFORMATION OWNER/OPR SIGNATURE</b> 	<b>18b. DATE</b> <i>(YYYYMMDD)</i>
<b>19. ISSO ORGANIZATION/DEPARTMENT</b> LEAVE BLANK	<b>19b. ISSO OR APPOINTEE SIGNATURE</b> 	<b>19c. DATE</b> <i>(YYYYMMDD)</i>
<b>19a. PHONE NUMBER</b>		

**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

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



# DEFENSE COUNTERINTELLIGENCE AND SECURITY AGENCY

## INDUSTRY SAAR EXAMPLE

**UNCLASSIFIED**

SYSTEM AUTHORIZATION ACCESS REQUEST (SAAR)		OMB No. 0704-0630 OMB Approval expires: 20250631
<small>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 <a href="mailto:via-fo-iaac.esd.nbr.dod-information-collections@mail.mil">via-fo-iaac.esd.nbr.dod-information-collections@mail.mil</a>. 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.</small>		
<b>PRIVACY ACT STATEMENT</b>		
<small>AUTHORITY: Executive Order 13450; and Public Law 99-474, the Computer Fraud and Abuse Act</small>		
<small>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</small>		
<small>ROUTINE USE(S): None.</small>		
<small>DISCLOSURE: Disclosure of this information is voluntary; however, failure to provide the requested information may impede, delay or prevent further processing of this request.</small>		
<b>TYPE OF REQUEST</b>		<b>DATE (YYYYMMDD)</b>
INITIAL <input type="checkbox"/> USER ID LEAVE BLANK		20221229
<b>SYSTEM NAME (Platform or Applications)</b>		<b>LOCATION (Physical Location of System)</b>
NISP Enterprise Mission Assurance Support Service		NOT APPLICABLE
<b>PART I (To be completed by Requester)</b>		
<b>1. NAME (Last, First, Middle Initial)</b>		<b>2. ORGANIZATION</b>
DOE, JOHN		COMPANY ABC
<b>3. OFFICE SYMBOL/DEPARTMENT</b>		<b>4. PHONE (DSN or Commercial)</b>
SECURITY OFFICE		555-555-5555
<b>5. OFFICIAL E-MAIL ADDRESS</b>		<b>6. JOB TITLE AND GRADE/RANK</b>
JOHN.DOE@ABC.COM		INFORMATION SYSTEMS SECURITY MANAGER
<b>7. OFFICIAL MAILING ADDRESS</b>		<b>8. CITIZENSHIP</b>
123 EMASS LANE BOSTON, MA 02108		<input checked="" type="checkbox"/> US <input type="checkbox"/> FN <input type="checkbox"/> OTHER
		<b>9. DESIGNATION OF PERSON</b>
		<input type="checkbox"/> MILITARY <input type="checkbox"/> CIVILIAN <input checked="" type="checkbox"/> CONTRACTOR
<b>10. IA TRAINING AND AWARENESS CERTIFICATION REQUIREMENTS (Complete as required for user or functional level access.)</b>		
<input checked="" type="checkbox"/> I have completed the Annual Cyber Awareness Training. DATE (YYYYMMDD) 20221201		
<b>11. USER SIGNATURE</b>		<b>12. DATE (YYYYMMDD)</b>
SIGNATURE OF REQUESTOR		20221229
<b>PART II ENDORSEMENT OF ACCESS BY INFORMATION OWNER, USER SUPERVISOR OR GOVERNMENT SPONSOR</b> <small>(If individual is a contractor - provide company name, contract number, and date of contract expiration in Block 15.)</small>		
<b>13. JUSTIFICATION FOR ACCESS</b>		
1. CAGE CODE(S): 12345		
2. ASSIGNED ISSP: ISSP JANE SMITH		
3. REQUESTED ROLE(S): IAM		
<b>14. TYPE OF ACCESS REQUESTED</b>		
<input checked="" type="checkbox"/> AUTHORIZED <input type="checkbox"/> PRIVILEGED		
<b>15. USER REQUIRES ACCESS TO:</b> <input type="checkbox"/> UNCLASSIFIED <input type="checkbox"/> CLASSIFIED (Specify category)		
<input checked="" type="checkbox"/> OTHER NATIONAL INDUSTRIAL SECURITY PROGRAM ENTERPRISE MISSION ASSURANCE SUPPORT SERVICE		
<b>16. VERIFICATION OF NEED TO KNOW</b>		<b>16a. ACCESS EXPIRATION DATE (Contractors must specify Company Name, Contract Number, Expiration Date. Use Block 21 if needed.)</b>
<input checked="" type="checkbox"/> I certify that this user requires access as requested.		NOT APPLICABLE
<b>17. SUPERVISOR'S NAME (Print Name)</b>		<b>17a. SUPERVISOR'S EMAIL ADDRESS</b>
FSO - JOE BLOGGS		JOE.BLOGGS@ABC.COM
<b>17b. PHONE NUMBER</b>		555-555-5555
<b>17c. SUPERVISOR'S ORGANIZATION/DEPARTMENT</b>		<b>17d. SUPERVISOR SIGNATURE</b>
ABC SECURITY OFFICE		SIGNATURE OF FSO AND/OR KMP
		<b>17e. DATE (YYYYMMDD)</b>
		20221229
<b>18. INFORMATION OWNER/OPR PHONE NUMBER</b>		<b>18a. INFORMATION OWNER/OPR SIGNATURE</b>
LEAVE BLANK		
<b>18b. DATE (YYYYMMDD)</b>		
<b>19. ISSO ORGANIZATION/DEPARTMENT</b>		<b>19b. ISSO OR APPOINTEE SIGNATURE</b>
LEAVE BLANK		
<b>19c. DATE (YYYYMMDD)</b>		
<b>19a. PHONE NUMBER</b>		

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 NISP eMASS: <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

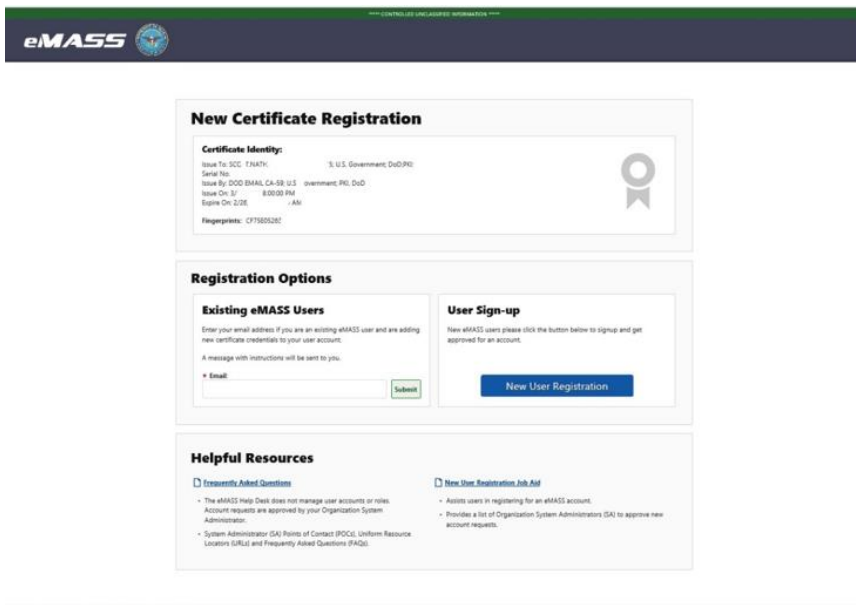
You are accessing a U.S. Government (USG) Information System (IS) that is provided for USG-authorized use only. By using this IS (which includes any device attached to this IS), you consent to the following conditions:

- 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. Click [Next Step]. **Note: If the CAGE Code is not available, please contact the DCSA NISP eMASS Team at [dcsa.quantico.dcsa.mbx.emass@mail.mil](mailto:dcsa.quantico.dcsa.mbx.emass@mail.mil).**

**New eMASS Account Registration**

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

\* Organization: [Dropdown Menu] Account Request Comments: [Text Area]

Cancel Next Step

**Certificate Identity:**

Issue To: [Redacted] U.S. Government OIG/DO  
Serial No: [Redacted]  
Issue By: OIG (EMAIL, CA-59) U.S. Government, FBI, DoD  
Issue On: 7/10/2019 8:09:00 PM  
Expires On: 7/10/2019 10:48:19 AM  
Fingerprints: [Redacted]

**Helpful Resources**

- [Frequently Asked Questions](#)
  - The eMASS Help Desk does not manage user accounts or roles. Account requests are approved by your Organization System Administrator.
  - System Administrator (SA) Points of Contact (POC), Uniform Resource Locations (URL) and Frequently Asked Questions (FAQ).
- [New User Registration Job Aid](#)
  - Assists users in registering for an eMASS account.
  - Provides a list of Organization System Administrators (SA) to approve new account requests.

- 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].

**New eMASS Account Registration**

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

**Account Details for Organization:** [Redacted]

**Personal Information**

\* First Name: NATHAN Middle Initial: [Redacted] \* Last Name: SCOTT

\* Phone: [Redacted]

Title: [Redacted]

Position: [Redacted]

\* Email: [Redacted]

**Notification Preferences**

**Date Approaching (Daily message, as date approaches)**

- System Authorization Termination Date Approaching
- POA&M Item Scheduled Completion Date Approaching

**Update Notifications**

- System Update Summary (POA&M Item, Artifact, Security Control Status)
- System Authorization Granted
- Critical Security Control Compliance Update

**Workload Tasks**

Workload Task Summary Frequency: Never [Dropdown]

Immediate Workload Task Emails: Yes [Dropdown]

Back Submit



- 5. In the Documentation step, Industry will upload all NISP eMASS user account documentation. **Note: Users must zip their pre-requisites into a single folder prior to uploading.**

(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 eMASS Team at [dcsa.quantico.dcsa.mbx.emass@mail.mil](mailto: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](#)

- 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.

**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 NISP 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](mailto: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 NISP eMASS Team at [dcsa.quantico.dcsa.mbx.emass@mail.mil](mailto: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 NISP 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 NISP eMASS Team ([dcsa.quantico.dcsa.mbx.emass@mail.mil](mailto:dcsa.quantico.dcsa.mbx.emass@mail.mil)) for system assignment.*