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: <u>https://cdse.usalearning.gov/login/index.php</u>
- 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)



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: <u>disa.meade.id.mbx.emass-tier-iii-support@mail.mil</u>

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".

DOD CYBER EXCHANGE PUBLIC		COVID-19	Topics	Training _U	PKI/PKE	SRGs/STIGs	Resources _	Help
	Cyber Awareness Challenge 2022 Version: 2022 / Length: 1 Hour							
Cyber Awareness Chailenge 2022	Launch Training							
ACCURATE ACCURATE	i totormation Cyber Awareness Challenge Couse Proview	The purpose of the Cyber Awareness users can engage to mitigate threats designed to be enging, and relevant standard for and user awareness tra- reauliments lased by Congress. It Defense, and Component input from ourse provides an overlevar d'auro- lasettied, controlle uncleastied in Check option is available for users w each selection on the indiget boats Cyber Awareness Challenge. If all ou any questions are answared incorrect incident.	s Challenge is and vulnerabil ining by procvi ining by procvi eo Office of Met to Do D C IO and st work. T ormation (CUI ho have succe users are pre- testions are an thy, users mus	to influence bet littles to DoD In The Cyber Awar ling awareness ing awareness ing awareness ing awareness ing awareness charted Cyber ity threats and the training also the t	navior, focusing, formation Syste reness Challeng content that add Budget (OMB). Workforces best videntifiable inf ad the previous nore questions d by, users will skip mplete all activit	on actions that au ms. This training is a is the DoD base dresses evolving the Office of the S isory Group (CV/2 b keep Information practices to prote formation (PII). A i version of the cou lerived from the pu to to the end of the ties contained with	chorized icurrent, ine ecretary of (G). This and set inowledge se. After revious incident. If win the	

- 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: <u>https://public.cyber.mil/help/</u>.



CDSE STEPP Site

- 1. Access the CDSE STEPP site: <u>https://cdse.usalearning.gov/login/index.php</u>
- 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



- 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.



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 (S	AAR) OMB No. 0704-0630 OMB approval expires: 20250531				
The public reporting burden for this collection of information, 0704-0530, is estimated to warage 5 minutes per response, including the time for reviewing instructions, searching estimating 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 estimation of the collection of information-collections@mail.mill.Respondents should be were that notwithstanding any other provision of law, no person shall be subject to any persety for dating to comply with a collection of information if it does not display a currently valid OMB control number.					
PRIVACY ACT TATEMENT AUTHORITY: Executive Order 19450; and Public Law 99-474, the Computer Fraud and Abuse Act PRINCIPAL PURPOSE(8): To record names, signatures, and other identifiers for the purpose of validating the fustworthines Defense (DoD) systems and information. NOTE: Records may be maintained in both electronic and/or paper form ROUTINE U3E(8): None. DISOLOSURE: Disclosure of this information is volunfary; however, failure to provide the requested information may impede.	s of individuals requesting access to Department of delay or prevent further processing of this request.				
TYPE OF REQUEST	DATE (YYYYMMDD)				
INITIAL USER ID LEAVE BLANK	20221229				
SYSTEM NAME (Platform or Applications) LOCATI	DN (Physical Location of System)				
NISP Enterprise Mission Assurance Support Service NOT A	PPLICABLE				



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.

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	8. CITIZENSHIP	9. DESIGNATION OF PERSON		
123 EMASS LANE	🗙 US 📃 FN	MILITARY CIVILIAN		
BOSTON, MA 02108	OTHER			
10. IA TRAINING AND AWARENESS CERTIFICATION REQUIREMENTS (Co	mplete as required for user or functional	level access.)		
I have completed the Annual Cyber Awareness Training. DATE	(VYYY)(MOD) 20221201			
11. USER SIGNATURE		12. DATE (YYYYMMOD)		
SIGNATURE OF REQUESTOR		20221229		



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. <u>CAGE CODE(s)</u>: 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. <u>REQUESTED ROLE(S)</u>: 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 <u>NOT</u> 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	N OWNER, USER SUPERVISOR OR GOVERNMENT SPON	ISOR
(if individual is a contractor - provide company name, contra	act number, and date of contract expiration in Block 10.)	
1. CAGE CODE(s) : 12345		
2 ASSIGNED ISSP - ISSP IANE SMITH		
3 REQUESTED ROLE(S): JAM		
14. TYPE OF ACCESS REQUESTED		
AUTHORIZED PRIVILEGED		
15. USER REQUIRES ACCESS TO: UNCLASSIFI	ED CLASSIFIED (Specify category)	
OTHER NATIONAL INDUSTRIAL SECU	RITY PROGRAM ENTERPRISE MISSION ASSUR	ANCE SUPPORT SERVICE
16. VERIFICATION OF NEED TO KNOW	16a. ACCESS EXPIRATION DATE (Contractors must spec	lly Company Name, Contract Number,
I certify that this user requires	Expiration Date. Use Block 21 If needed.)	
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 (YYYYMMOD)
LEAVE BLANK	(WRYAN)	
19. ISSO ORGANIZATION/DEPARTMENT	19b. ISSO OR APPOINTEE SIGNATURE	19c. DATE (YYYYMMDD)
LEAVE BLANK	Marked -	
19a. PHONE NUMBER]	

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 <u>EACH</u> 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

R) Instructions, searching exis Ion suggestions to the Dep rovision of law, no person notividualis requesting a		
instructions, searching esti for suggestions to the Dep revision of law; no person ndividuals requesting a	OU/B No. 0704-0530 OU/B approval expires: 20250631	
ndividuais requesting a	ting data sources, gathering and artment of Defense, Vilashington shall be subject to any penalty for	
or prevent further pro-	ccess to Department of	
er present some pre-	DATE (XXXXMMDD)	
	20221229	
Physical Location of	(System)	
ICABLE		
к		
SECURITY MAD	NAGER	
9. DESIGNA	TION OF PERSON	
MILIT	ARY CIVILIAN	
	TRACTOR	
ional level access.)		
12. DATE (M	YYYNNDD)	
	20221229	
SPONSOR		
SURANCE SUPP	ORT SERVICE	
specify Company N	lame, Contract Number,	
Explation Date. Use Block 21 if needed.)		
	NUMBER	
17b. PHONE	55	
17b. PHONE 555-555-55	YYYYMMDD)	
17b. PHONE 555-555-55 17e. DATE (1	20221229	
17b. PHONE 555-555-55 17e. DATE (1	YYYYMMDD)	
17b. PHONE 555-555-55 17e. DATE (
17b. PHONE 555-555-55 17e. DATE (18b. DATE (WWWWWWWWW	
17b. PHONE 555-555-55 17e. DATE (18b. DATE (18c. DATE (rrr ningerey	
17b. PHONE 555-555-55 17e. DATE (18b. DATE (18c. DATE (
	18b. DATE (

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: <u>https://nisp.emass.apps.mil</u>. 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.

eMA	\55 🛞	
	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:	THENT OF DE
	 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. 	5
	 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. 	THU STATES OF ANE
	 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 oMASS	

2. Select New User Registration.

A33	W	
	New Certificate Registration	
	Certificate Identity: Issue Ta SCC TANK: Issue Ta SCC TANK: Issue October 12, SCC 1	Q
	Registration Options	
	Existing eMASS Users Energion and address if you are in existing eMASS our and are adding new cardinate credentials tryour user ecourts. A message with instructions will be are to you.	User Sign-up New 40435 user planes thick the button below to signup and get approved for an account.
	Solonit	New User Registration
	Helpful Resources	
	The eMASS Help Desk does not manage user accounts or roles. Account requests are approved by your Organization System Account requests are approved by your Organization System	Next User Residuation, Job Add Add and Add Add Add Add Add Add Add Add Add A
	 System Administrator (SA) Points of Contact (POCs), Uniform Resource Locators (URLs) and Frequently Asked Questions (FAQs). 	account requests.



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.*

New eMASS Account Registration
1.0xyunintee 2.4mm/mill 1.2mm/mmill 4.4mm/mill 1.314.4mm/
Granization: Account Report Communit:
Certificate Identity: U.S. Government DoD/R: Provide the
Helpful Resources Traumit Adva Cuentina To a Add Sing: Deal does not many a guard and a start in signature for an Add Sing Deal does not any a signature of the add Sing Deal does for the provide Signature System Advancement (Add Name Advancement Counters Provide) System Advancement Counters Provide

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].

	1. Organization	2. Account Details	3. Documentation	4. Confirm Email	5. SA Approva	
_						
count De	tails for Org	anization:		No. of of a set of a set of a		
Personal Inte	ormation			Notification Prefer	ences	
 First Name: 	Middle I	nitial: * Last Name:		Date Approaching (Dail	y message, as dat	e approaches)
NATHAN		SCOTT		System Authorization Te	ermination Date Ap	proaching
Phone:		_		POA&M Item Schedule	d Completion Date	Approaching
		J		Update Notifications		
litle:				System Update Summa (POA&M Item, Artifact,	ry Security Control Sta	itus)
				System Authorization G	ranted	
osition:				Critical Security Control	Compliance Updat	e
				Workload Tasks		
Email:				Workload Task Summary	Frequency:	Never



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 <u>dcsa.quantico.dcsa.mbx.emass@mail.mil</u>.

	1. Organization	2. Account Details	3. Documentation	4. Confirm Email	5. SA Approval
Jploa	d User Acco	ount Docum	ientation		
Jploa lease upload rganizationa	d User Acco the appropriate access d I eMASS administrators w	Dunt Docum locument(s) that are requir when reviewing your accou	ed by your Organization. Th nt request. Please refer to t	hese documents will be ava he "New User Registration	ailable to your " Job Aid below

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.

	····· CONTROLLED UNCLESSING INVORMATION ·····
AASS 🎯	
	The user artifacts has been added successfully.
	New eMASS Account Registration
	1. Organization 2. Account Details 3. Decumentation 4. Confirm Email 5. SA Approval
	eMASS account is pending email verification.
	Please check your email and use the provided link to verify the address. Once verified, your administrator will be notified to review the request.
	seetes anal versions



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.



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 <u>dcsa.quantico.dcsa.mbx.emass@mail.mil</u>.

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 (<u>dcsa.quantico.dcsa.mbx.emass@mail.mil</u>) for system assignment.