Job Aid

INDUSTRY ONBOARDING PSSAR GUIDANCE

Updated Date: 02/2024	Product ID: KB0011418 V13
Organization Type: FSO	
User Roles(S): FSO	

TABLE OF CONTENTS

Purpose: To provide guidance on how to fill out the Personnel Security System Access Request (PSSAR) and how to avoid common errors made.

INDUSTRY ONBOARDING PSSAR GUIDANCE

Pre-Requisite to Access NBIS

The PSSAR specifically refers to the following courses:

- **Cyber Awareness Challenge/Security Training** with a course completion certificate.
  a. Non-CAC users: https://public.cyber.mil
  b. CAC users: https://cyber.mil
- **PII Training** with a course completion certificate.
  a. https://securityawareness.usalearning.gov/piiv2/index.htm

Personnel Security System Access Request Form

The PSSAR form, also known as DD Form 2962, is used by the Defense Counterintelligence and Security Agency (DCSA) to collect information required to grant access to personnel security systems, specifically the National Background Investigation Services (NBIS) system. PSSARs must be completed and maintained for all system users. Before access is granted, PSSARs must include the signatures of the individual requesting an account, the nominating official, and the validating official.

Use this guidance and the PSSAR form template provided in the NBIS Onboarding for NISP Contractor Request document to complete the form correctly.

Note:

- The applicant (requestor) is responsible for completing Parts 1-4.
- The nominating official, the individual who is authorizing that the applicant, should have the access requested, must be a Key Management Personnel (KMP) listed in NISS, a Facility Security Officer, or the Security Officer/Manager.
    - Users may submit one PSSAR for multiple CAGE codes if the signee in Part 5 is a KMP for all listed CAGE codes.
    - If there is not an overlapping KMP for multiple CAGE codes that can sign Part 5, separate PSSARs will be required.
    - Users may submit one PSSAR or multiple PSSARs as part of the same onboarding request in ServiceNow.
- The validating official (someone who can validate the investigation requirements) is responsible for completing Part 6.
- Find additional PSSAR instructions in Part 7 (the last page of the PSSAR form).
- The PSSAR will be submitted via the NBIS Onboarding for NISP Contractors Request in ServiceNow for only the initial NBIS organization and the user with the User Manager role.
    - Subsequent NBIS accounts will be provisioned by the User Manager(s).

- To ensure usage of the current PSSAR form, ensure the "OMB approval expires" date in the upper right corner of the first page of the form is beyond the current date and the lower left corner of each page lists "DD FORM 2962, Vol 2, JAN 2020."

A blank PSSAR form can be found at:
https://www.esd.whs.mil/Portals/54/Documents/DD/forms/dd/dd2962v2.pdf

How to Fill Out the Industry Onboarding PSSAR Template

The PSSAR can be used to request new accounts, make modifications to an existing account, or to deactivate an active account.

1. Part 1 of the PSSAR form is to be completed by the applicant who inputs his/her **personal information.**

Note:

- Part 1, Block 3 requests putting the top-level SMO name in DISS that access is needed for to ensure proper provisioning into the NBIS organization based on data migration.
- Part 1, Block 5 will receive automated emails from donotreply@nbis.mil to complete NBIS enrollment. Make sure to provide an email address that is actively monitored and can receive automated emails.

CUI (when filled in)

Name *(Last, First, Middle Initial)*: Last, First, MI

PERSONNEL SECURITY SYSTEM ACCESS REQUEST (PSSAR)
DEFENSE COUNTERINTELLIGENCE AND SECURITY AGENCY (DCSA)

OMB No. 0705-0009
OMB approval expires 20250131

The public reporting burden for this collection of information, 0704-0542, is estimated to average 10 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. PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ADDRESS. Return completed form to the appropriate Account Manager or DCSA Contact Center, as indicated in the instructions.

PRIVACY ACT STATEMENT

AUTHORITY: E.O. 12829, National Industrial Security Program; E.O. 10450, Security Requirements for Government Employment; E.O. 10865, Safeguarding Classified Information Within Industry; (DoDI) 1400.25, Volume 731, DoD Civilian Personnel Management System: Suitability and Fitness Adjudication for Civilian Employees; DoDM 5200.02, Procedures for the DoD Personnel Security Program; DoDI 5200.02, DoD Personnel Security Program (PSP); DoDD 5220.6, Defense Industrial Personnel Security Clearance Review Program; DoDI 5220.22, National Industrial Security Program (NISP); DoDI 5200.46, DoD Investigative and Adjudicative Guidance for Issuing the Common Access Card (CAC); Homeland Security Presidential Directive (HSPD) 12, Policy for Common Identification Standard for Federal Employees and Contractors; and E.O. 9397 (SSN), as amended.

PURPOSE(S): To request the establishment of user roles and access and validate the trustworthiness of individuals seeking access to Defense Central Index of Investigations (DCII), DoD Secure Web Fingerprint Transmission (SWFT), DoD Defense Information system for Security (DISS) or National Background Investigation Services (NBIS).

ROUTINE USE(S): Disclosure of records are generally permitted under 5 U.S.C. 552a(b) of the Privacy Act of 1974, as amended. See the appropriate System of Records Notice for the applicable routine uses: A complete list of the routine uses can be found in the system of records notice for the Department of Defense Personnel Vetting Records System, "DUSDI 02-DoD" at: https://www.federalregister.gov/documents/2018/10/17/2018-22508/privacy-act-of-1974-system-of-records; DUSDI 02-DoD, Personnel Vetting Records System at: http://dpcld.defense.gov/Privacy/SORNsIndex/DOD-Component-Notices/OSDJS-Article-List/

DISCLOSURE: Voluntary. However failure to provide the requested information may impede, delay, or prevent further processing of your request. The Social Security Number is used to verify the trustworthiness status.

PART 1 - PERSONAL INFORMATION

1. NAME *(Last, First, Middle Initial)*	2. ORGANIZATION	
Last, First, MI of applicant (if no middle initial enter NMN)	Employing Organization or Company Name of applicant	
3. OFFICE SYMBOL / DEPARTMENT	4. PHONE *(DSN or Commercial)*	
Top Level SMO Name as it appears in DISS	Telephone number of applicant	
5. OFFICIAL E-MAIL ADDRESS	6. JOB TITLE AND GRADE/RANK	
Official email of applicant to be used for account creation	Job title	
7. OFFICIAL MAILING ADDRESS	8. CITIZENSHIP	9. DATE OF BIRTH *(YYYYMMDD)*
Official mailing address of applicant	Lisa all countries of citizenship	Date of Birth of applicant
10. PLACE OF BIRTH *(City & State/Country)*	11. SOCIAL SECURITY NUMBER	12. CAGE CODE *(CTR Only)*
City, State if born in U.S. otherwise City, Country	SSN is required XXX-XX-XXXX	Org CAGE code from DISS

13. DESIGNATION OF APPLICANT ☐ MILITARY ☐ DoD CIVILIAN ☑ INDUSTRY ☐ NON-DoD

Complete Part 2, Block 19 of the PSSAR form requesting NBIS system access for the applicant.

2. Select **initial** for a new account, **modification** to change privileges to an existing account, or **deactivate** to remove all access and disable an account.

Note:

- In 19a, the roles listed are based on various organization types. Not all are currently available in NBIS. We encourage users to ignore block 19a and put all roles requested into 19b.
    - For Industry users to manage organizations, users, and configurations and to be able to submit investigations, the initial user(s) should request the following roles: Org Manager, User Manager, Notification Manager, Workflow Manager, Reviewer, Facility Security Officer, and Task Reassignment.
    - There are additional roles available to Industry users, which are not essential to all organizations, but may be beneficial. These roles are Order Form Template Manager, Org Assignment Manager, Org Workload Manager, Program Tag Manager, and Subject Viewer.

Note: This form is used to request access for multiple systems. As such, Part 2, Section 19 applies to and is applicable for NBIS system access. For guidance on filling out the sections for other systems, please contact the System Representative.

19. NATIONAL BACKGROUND INVESTIGATION SERVICES (NBIS)

TYPE OF REQUEST

☑ INITIAL ☐ MODIFICATION ☐ DEACTIVATE

a. ROLE REQUESTED:

☐ SYSTEM MANAGER	☐ AUTHORIZER (GOVERNMENT ONLY)	☐ WORKFLOW MANAGER	☐ BUSINESS PROCESS MANAGER
☐ INTERNAL ORG MANAGER	☐ NBIS FINANCIAL MANAGER	☐ INITIATOR	☐ ORG MANAGER
☐ WORKLOAD MANAGER	☐ FINANCIAL MANAGER	☐ POINT OF CONTACT	☐ REVIEWER
☐ USER MANAGER	☐ INTERNAL USER MANAGER	☐ NOTIFICATION MANAGER	☐ ORDER FORM TEMPLATE MANAGER
☐ OTHER			

b. LIST ANY ELEVATED PERMISSIONS:

Initial Industry user of an organization should request the following roles:
Org Manager
User Manager
Notification Manager
Workflow Manager
Reviewer
Facility Security Officer (FSO)
Task Reassignment

3. Complete Part 3 by entering the applicant's **completion date** for required Cyber Awareness and Personally Identifiable Information trainings.

Note: The training certificates also need to be provided with the PSSAR submission. The NBIS System Disclosure Agreement includes an acknowledgement that the user has "completed the necessary training with regards to Security Awareness and Safe-Guarding Personally Identifiable Information (PII)."

PART 3 - TRAINING *(I have completed and attached training certificates for):*			
20. ☑ CYBER AWARENESS TRAINING		**DATE** *(YYYYMMDD)*	Enter date of completion
21. ☑ PERSONALLY IDENTIFIABLE INFORMATION TRAINING		**DATE** *(YYYYMMDD)*	Enter date of completion

4. Part 4 requires the applicant submit a **signature** acknowledging system policies.

PART 4 - APPLICANT'S CERTIFICATION	
I hereby certify that I understand that by signing this Personnel Security System Access Request, I am solely responsible for the use and protection of the account that I will be provided. I also understand that I am not authorized to share my account or logon credentials with any other individuals. I will utilize all tools and applications in accordance with the account management policy and security policy, as well as all applicable U.S. laws and DoD regulations. I understand that if I violate any account management policy, security policy, U.S. laws or DoD regulations, my account will immediately be terminated, and may be subject to criminal charges and penalties.	
22. APPLICANT'S SIGNATURE	**23. DATE** *(YYYYMMDD)*

5. For Part 5, provide a nominating official's **certification**.

Note: The nominating official is the individual who is authorizing that the applicant should have the access requested. The nominating official must be:

- Key Management Personnel (KMP) listed in the National Industrial Security System (NISS).
- The organization's Facility Security Officer, Security Officer, or Security Manager.
- The nominating official cannot be the same as the applicant unless the organization is a single person facility.

PART 5 - NOMINATING OFFICIAL'S CERTIFICATION		
24. I certify that the above named individual meets the requirements for access, has the appropriate need-to-know, and if applicable, meets the requirements for account management privileges. I am also aware that I am responsible for ensuring this individual will follow all account policies, security policies, and all applicable DoD regulations and U.S. laws. Furthermore, I certify that the named applicant requires account access as indicated above in order to perform assigned duties.		
25. NOMINATING OFFICIAL'S PRINTED NAME *(Last, First, Middle Initial)*	**26. NOMINATING OFFICIAL'S TITLE**	
Last, First, MI of Nominating Official	Title of Nominating Official	
27. NOMINATING OFFICIAL'S TELEPHONE NUMBER	**28. NOMINATING OFFICIAL'S SIGNATURE**	**29. NOMINATING OFFICIAL'S SIGNATURE DATE**
Telephone number of Nominating Official; enter DSN or Commercial		

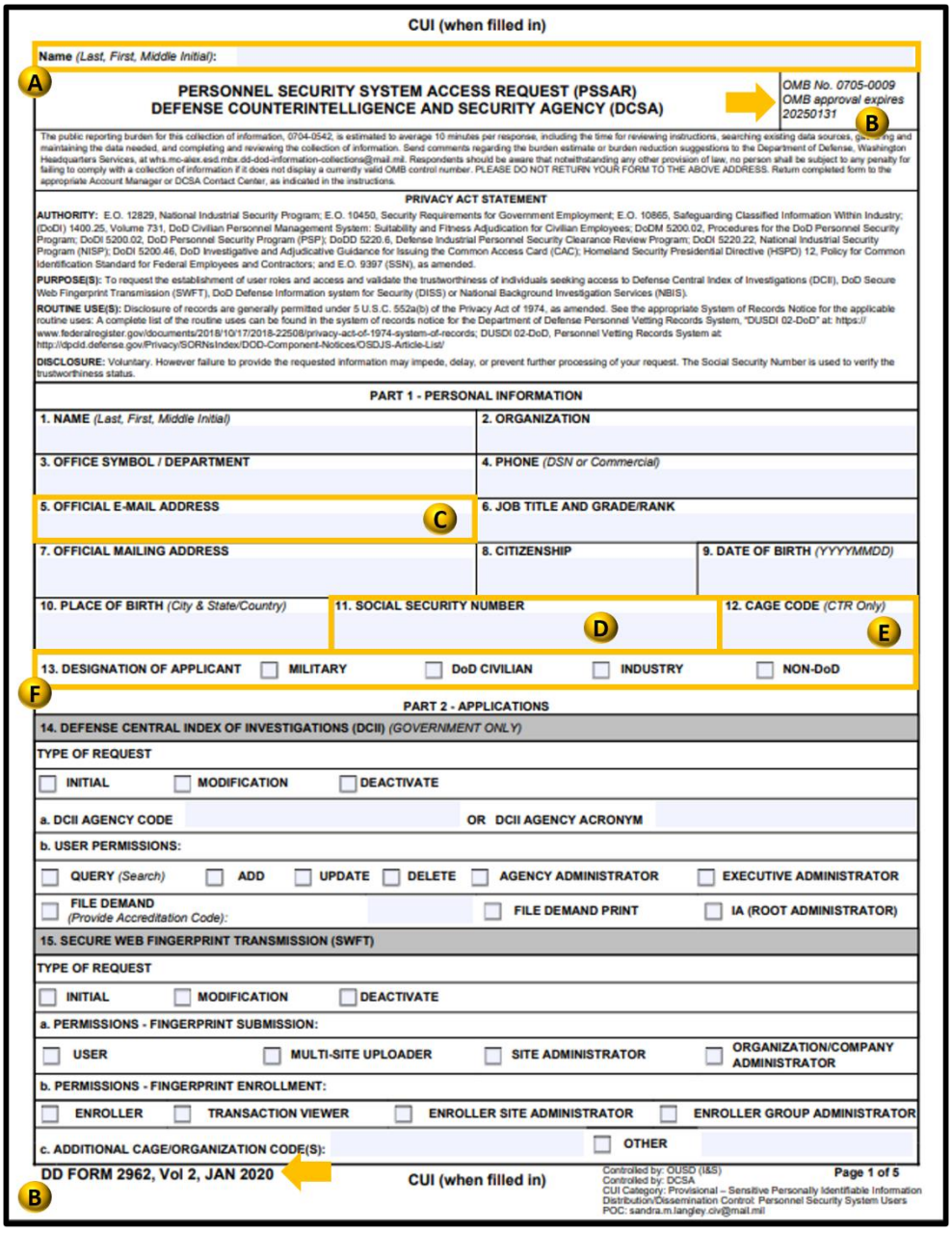
6. For Part 6, provide the validating official's **verification**.

Note: For non-DoD government agency requests, the Chief of Security or designee must complete this section. This section will not be completed if self-nominating/validating.

PART 6 - VALIDATING OFFICIAL'S VERIFICATION			
I have verified that minimum investigative requirements for the above applicant have been met and the applicant has the necessary need-to-know to access the personnel security systems requested.			
30. ELIGIBILITY/ACCESS LEVEL:	Eligibility/Access level of applicant	**31. TYPE OF INVESTIGATION:**	Type of Investigation completed
32. ELIGIBILITY GRANTED DATE:	Clearance granted or interim started	**33. DATE INVESTIGATION COMPLETED:**	
34. ELIGIBILITY ISSUED BY:	Organization that issued clearance	**35. INVESTIGATION CONDUCTED BY:**	Investigating Agency
36. VALIDATING OFFICIAL'S PRINTED NAME *(Last, First, Middle Initial):*			
Last, First, MI			
37. VALIDATING OFFICIAL'S SIGNATURE *(Last, First, Middle Initial):*		**38. VALIDATING OFFICIAL'S SIGNATURE DATE**	

Common PSSAR Completion Errors

A. Omission of the applicant's name on each page header. The applicant's name must be listed at the top of each page submitted in the format: Last, First, Middle Initial.
B. Using an outdated form. Make sure the date in the upper right corner of the first page is beyond the current date and the lower left corner of each page lists "DD Form 2962, Vol 2, Jan 2020."
C. Part 1 Block 5: Personal email address being entered instead of an official email address.
D. Part 1 Block 11: An incomplete Social Security number.
E. Part 1 Block 12: This field is for contractors only and the issue here is the omission of a CAGE code; likely due to the information not being known by the applicant.
F. Part 1 Block 13: Omission or incorrect designation of the applicant.



CUI (when filled in)

Name *(Last, First, Middle Initial)*:

PERSONNEL SECURITY SYSTEM ACCESS REQUEST (PSSAR)
DEFENSE COUNTERINTELLIGENCE AND SECURITY AGENCY (DCSA)

OMB No. 0705-0009
OMB approval expires 20250131

The public reporting burden for this collection of information, 0704-0542, is estimated to average 10 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. PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ADDRESS. Return completed form to the appropriate Account Manager or DCSA Contact Center, as indicated in the instructions.

PRIVACY ACT STATEMENT

AUTHORITY: E.O. 12829, National Industrial Security Program; E.O. 10450, Security Requirements for Government Employment; E.O. 10865, Safeguarding Classified Information Within Industry; (DoDI) 1400.25, Volume 731, DoD Civilian Personnel Management System: Suitability and Fitness Adjudication for Civilian Employees; DoDM 5200.02, Procedures for the DoD Personnel Security Program; DoDI 5200.02, DoD Personnel Security Program (PSP); DoDD 5220.6, Defense Industrial Personnel Security Clearance Review Program; DoDI 5220.22, National Industrial Security Program (NISP); DoDI 5200.46, DoD Investigative and Adjudicative Guidance for Issuing the Common Access Card (CAC); Homeland Security Presidential Directive (HSPD) 12, Policy for Common Identification Standard for Federal Employees and Contractors; and E.O. 9397 (SSN), as amended.

PURPOSE(S): To request the establishment of user roles and access and validate the trustworthiness of individuals seeking access to Defense Central Index of Investigations (DCII), DoD Secure Web Fingerprint Transmission (SWFT), DoD Defense Information system for Security (DISS) or National Background Investigation Services (NBIS).

ROUTINE USE(S): Disclosure of records are generally permitted under 5 U.S.C. 552a(b) of the Privacy Act of 1974, as amended. See the appropriate System of Records Notice for the applicable routine uses: A complete list of the routine uses can be found in the system of records notice for the Department of Defense Personnel Vetting Records System, "DUSDI 02-DoD" at: https://www.federalregister.gov/documents/2018/10/17/2018-22508/privacy-act-of-1974-system-of-records; DUSDI 02-DoD, Personnel Vetting Records System at http://dpcld.defense.gov/Privacy/SORNsIndex/DOD-Component-Notices/OSDJS-Article-List/

DISCLOSURE: Voluntary. However failure to provide the requested information may impede, delay, or prevent further processing of your request. The Social Security Number is used to verify the trustworthiness status.

PART 1 - PERSONAL INFORMATION

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	9. DATE OF BIRTH *(YYYYMMDD)*
10. PLACE OF BIRTH *(City & State/Country)*	11. SOCIAL SECURITY NUMBER	12. CAGE CODE *(CTR Only)*

13. DESIGNATION OF APPLICANT ☐ MILITARY ☐ DoD CIVILIAN ☐ INDUSTRY ☐ NON-DoD

PART 2 - APPLICATIONS

14. DEFENSE CENTRAL INDEX OF INVESTIGATIONS (DCII) *(GOVERNMENT ONLY)*

TYPE OF REQUEST

☐ INITIAL ☐ MODIFICATION ☐ DEACTIVATE

a. DCII AGENCY CODE OR DCII AGENCY ACRONYM

b. USER PERMISSIONS:

☐ QUERY *(Search)* ☐ ADD ☐ UPDATE ☐ DELETE ☐ AGENCY ADMINISTRATOR ☐ EXECUTIVE ADMINISTRATOR

☐ FILE DEMAND *(Provide Accreditation Code)*: ☐ FILE DEMAND PRINT ☐ IA (ROOT ADMINISTRATOR)

15. SECURE WEB FINGERPRINT TRANSMISSION (SWFT)

TYPE OF REQUEST

☐ INITIAL ☐ MODIFICATION ☐ DEACTIVATE

a. PERMISSIONS - FINGERPRINT SUBMISSION:

☐ USER ☐ MULTI-SITE UPLOADER ☐ SITE ADMINISTRATOR ☐ ORGANIZATION/COMPANY ADMINISTRATOR

b. PERMISSIONS - FINGERPRINT ENROLLMENT:

☐ ENROLLER ☐ TRANSACTION VIEWER ☐ ENROLLER SITE ADMINISTRATOR ☐ ENROLLER GROUP ADMINISTRATOR

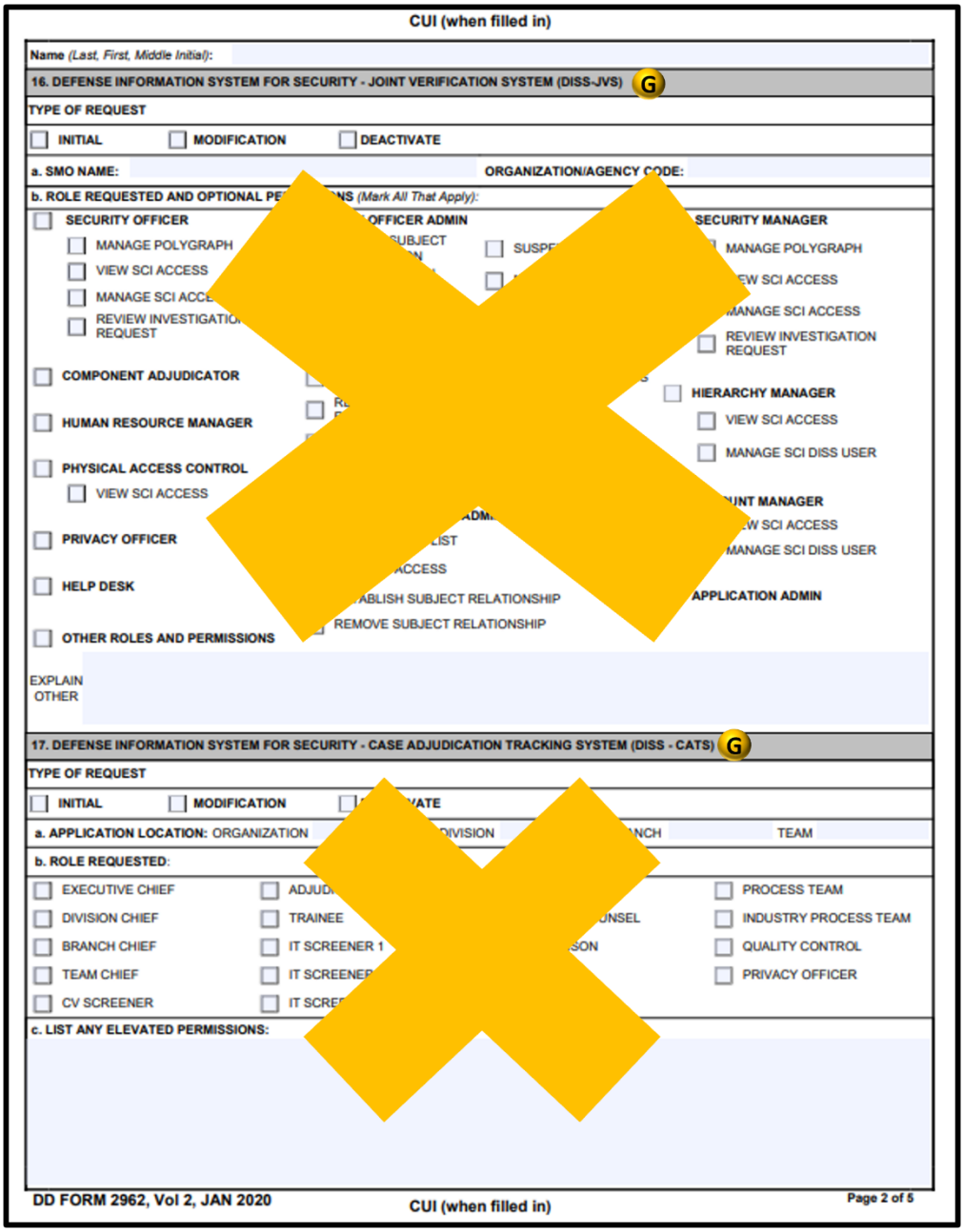
c. ADDITIONAL CAGE/ORGANIZATION CODE(S): ☐ OTHER

DD FORM 2962, Vol 2, JAN 2020 CUI (when filled in)

Controlled by: OUSD (I&S)
Controlled by: DCSA
CUI Category: Provisional – Sensitive Personally Identifiable Information
Distribution/Dissemination Control: Personnel Security System Users
POC: sandra.m.langley.civ@mail.mil

Page 1 of 5

G. Part 2: Requesting access to another system besides NBIS.



CUI (when filled in)

Name *(Last, First, Middle Initial)*:

16. DEFENSE INFORMATION SYSTEM FOR SECURITY - JOINT VERIFICATION SYSTEM (DISS-JVS) G

TYPE OF REQUEST

☐ INITIAL ☐ MODIFICATION ☐ DEACTIVATE

a. SMO NAME: ORGANIZATION/AGENCY CODE:

b. ROLE REQUESTED AND OPTIONAL PE NS *(Mark All That Apply)*:

☐ SECURITY OFFICER
- ☐ MANAGE POLYGRAPH
- ☐ VIEW SCI ACCESS
- ☐ MANAGE SCI ACCE
- ☐ REVIEW INVESTIGATIO REQUEST

☐ COMPONENT ADJUDICATOR

☐ HUMAN RESOURCE MANAGER

☐ PHYSICAL ACCESS CONTROL
- ☐ VIEW SCI ACCESS

☐ PRIVACY OFFICER

☐ HELP DESK

☐ OTHER ROLES AND PERMISSIONS

☐ OFFICER ADMIN
- ☐ SUBJECT N
- ☐ SUSPE
- ☐ R

ACCESS
- ABLISH SUBJECT RELATIONSHIP
- ☐ REMOVE SUBJECT RELATIONSHIP

☐ SECURITY MANAGER
- ☐ MANAGE POLYGRAPH
- ☐ EW SCI ACCESS
- ☐ ANAGE SCI ACCESS
- ☐ REVIEW INVESTIGATION REQUEST

☐ HIERARCHY MANAGER
- ☐ VIEW SCI ACCESS
- ☐ MANAGE SCI DISS USER

☐ INT MANAGER
- ☐ W SCI ACCESS
- ☐ MANAGE SCI DISS USER

☐ APPLICATION ADMIN

EXPLAIN OTHER

17. DEFENSE INFORMATION SYSTEM FOR SECURITY - CASE ADJUDICATION TRACKING SYSTEM (DISS - CATS) G

TYPE OF REQUEST

☐ INITIAL ☐ MODIFICATION ☐ VATE

a. APPLICATION LOCATION: ORGANIZATION DIVISION NCH TEAM

b. ROLE REQUESTED:

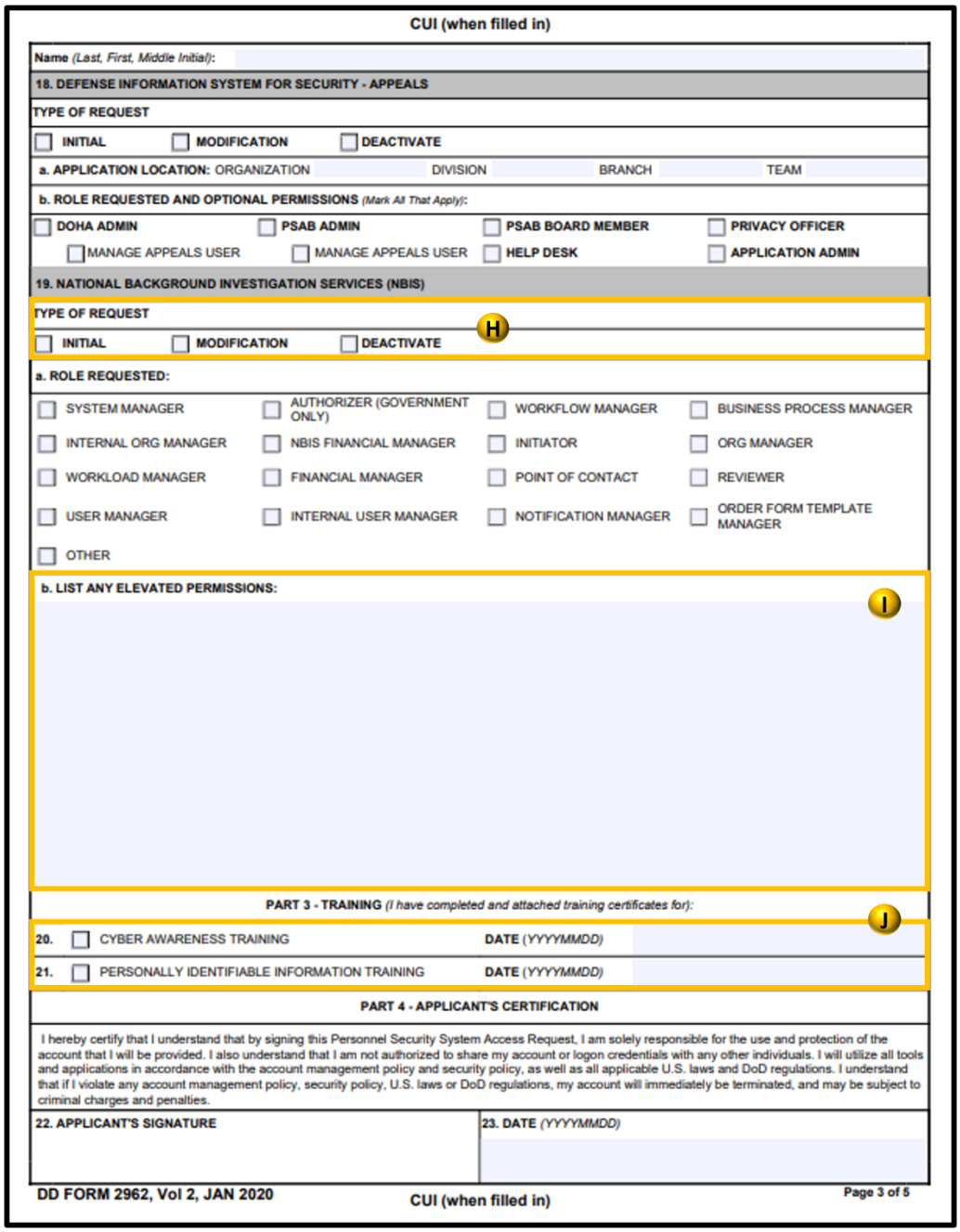
☐ EXECUTIVE CHIEF	☐ ADJUD	☐ PROCESS TEAM
☐ DIVISION CHIEF	☐ TRAINEE	☐ INDUSTRY PROCESS TEAM
☐ BRANCH CHIEF	☐ IT SCREENER 1	☐ QUALITY CONTROL
☐ TEAM CHIEF	☐ IT SCREENER	☐ PRIVACY OFFICER
☐ CV SCREENER	☐ IT SCRE	

UNSEL
SON

c. LIST ANY ELEVATED PERMISSIONS:

DD FORM 2962, Vol 2, JAN 2020 CUI (when filled in) Page 2 of 5

H. Part 2: The user has already been provisioned in the current and/or parent organization.
I. Part 2 Block 19B: This is a free-text field. Often, the entity requesting access already fills this out for the applicant. A common error seen here is a failure to list content in the Org Name or Org Code sections. Another common error is when the user requests an Authorizer role on behalf of a Contractor, which is not allowed.
J. Part 3: The omission of or incorrect training certificate dates, as well as the submission of Non-DOD Cyber Awareness and or PII Certifications.



CUI (when filled in)

Name *(Last, First, Middle Initial)*:

18. DEFENSE INFORMATION SYSTEM FOR SECURITY - APPEALS

TYPE OF REQUEST

☐ INITIAL ☐ MODIFICATION ☐ DEACTIVATE

a. APPLICATION LOCATION: ORGANIZATION DIVISION BRANCH TEAM

b. ROLE REQUESTED AND OPTIONAL PERMISSIONS *(Mark All That Apply)*:

☐ DOHA ADMIN ☐ PSAB ADMIN ☐ PSAB BOARD MEMBER ☐ PRIVACY OFFICER
☐ MANAGE APPEALS USER ☐ MANAGE APPEALS USER ☐ HELP DESK ☐ APPLICATION ADMIN

19. NATIONAL BACKGROUND INVESTIGATION SERVICES (NBIS)

TYPE OF REQUEST

H

☐ INITIAL ☐ MODIFICATION ☐ DEACTIVATE

a. ROLE REQUESTED:

☐ SYSTEM MANAGER ☐ AUTHORIZER (GOVERNMENT ONLY) ☐ WORKFLOW MANAGER ☐ BUSINESS PROCESS MANAGER
☐ INTERNAL ORG MANAGER ☐ NBIS FINANCIAL MANAGER ☐ INITIATOR ☐ ORG MANAGER
☐ WORKLOAD MANAGER ☐ FINANCIAL MANAGER ☐ POINT OF CONTACT ☐ REVIEWER
☐ USER MANAGER ☐ INTERNAL USER MANAGER ☐ NOTIFICATION MANAGER ☐ ORDER FORM TEMPLATE MANAGER
☐ OTHER

b. LIST ANY ELEVATED PERMISSIONS:

I

PART 3 - TRAINING *(I have completed and attached training certificates for)*:

J

20. ☐ CYBER AWARENESS TRAINING **DATE** *(YYYYMMDD)*
21. ☐ PERSONALLY IDENTIFIABLE INFORMATION TRAINING **DATE** *(YYYYMMDD)*

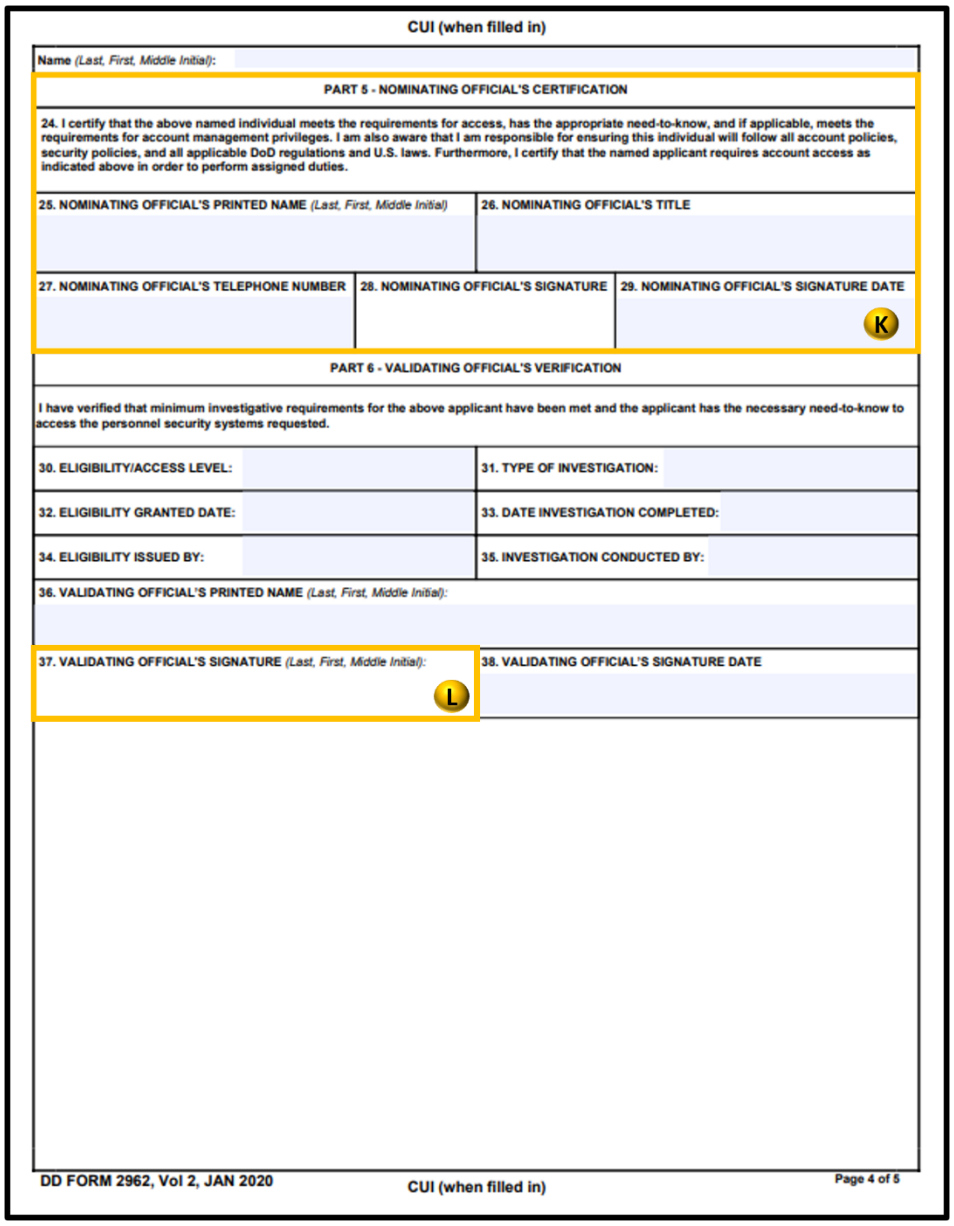
PART 4 - APPLICANT'S CERTIFICATION

I hereby certify that I understand that by signing this Personnel Security System Access Request, I am solely responsible for the use and protection of the account that I will be provided. I also understand that I am not authorized to share my account or logon credentials with any other individuals. I will utilize all tools and applications in accordance with the account management policy and security policy, as well as all applicable U.S. laws and DoD regulations. I understand that if I violate any account management policy, security policy, U.S. laws or DoD regulations, my account will immediately be terminated, and may be subject to criminal charges and penalties.

22. APPLICANT'S SIGNATURE | 23. DATE *(YYYYMMDD)*

DD FORM 2962, Vol 2, JAN 2020 CUI (when filled in) Page 3 of 5

K. Part 5: The nominating official is not a KMP and/or the omission of the nominating official's signature.
L. Part 6: The omission of the validating official's signature.



CUI (when filled in)

Name *(Last, First, Middle Initial)*:

PART 5 - NOMINATING OFFICIAL'S CERTIFICATION

24. I certify that the above named individual meets the requirements for access, has the appropriate need-to-know, and if applicable, meets the requirements for account management privileges. I am also aware that I am responsible for ensuring this individual will follow all account policies, security policies, and all applicable DoD regulations and U.S. laws. Furthermore, I certify that the named applicant requires account access as indicated above in order to perform assigned duties.

25. NOMINATING OFFICIAL'S PRINTED NAME *(Last, First, Middle Initial)*	26. NOMINATING OFFICIAL'S TITLE	
27. NOMINATING OFFICIAL'S TELEPHONE NUMBER	28. NOMINATING OFFICIAL'S SIGNATURE	29. NOMINATING OFFICIAL'S SIGNATURE DATE

K

PART 6 - VALIDATING OFFICIAL'S VERIFICATION

I have verified that minimum investigative requirements for the above applicant have been met and the applicant has the necessary need-to-know to access the personnel security systems requested.

30. ELIGIBILITY/ACCESS LEVEL:	31. TYPE OF INVESTIGATION:
32. ELIGIBILITY GRANTED DATE:	33. DATE INVESTIGATION COMPLETED:
34. ELIGIBILITY ISSUED BY:	35. INVESTIGATION CONDUCTED BY:

36. VALIDATING OFFICIAL'S PRINTED NAME *(Last, First, Middle Initial)*:

37. VALIDATING OFFICIAL'S SIGNATURE *(Last, First, Middle Initial)*:	38. VALIDATING OFFICIAL'S SIGNATURE DATE

L

DD FORM 2962, Vol 2, JAN 2020 CUI (when filled in) Page 4 of 5