Defense Counterintelligence and Security Agency

Personnel Security & Assurance

Defense Central Index of Investigations (DCII) Account Request Procedures

Document Version 3.0

March 14, 2022

Table of Contents

1 New DCII Agency (Site) Request

If a new Agency is required for using DCII, follow the steps listed below:

- Submit a DCII Agency Request form using your agency's letterhead and indicate your reasons for requesting a new DCII Agency to the DCSA Contact Center.
- Your agency Director or validated delegate must sign the request form. Delegates must be GS-14 grade (or military branch equivalent) or higher. To obtain a DCII Agency request template, navigate to the DCSA PSA DCII website (Defense Counterintelligence and Security Agency > Information Systems > Defense Central Index of Investigations (DCII) (dcsa.mil) select "Access request" and 'DCII Agency Request Form'. **NOTE**: DCII accounts will only be granted to U.S. Government agencies.
- Once approved you will be notified the new agency account has been created and provided an agency code/acronym for use on the PSSAR form. See Section 4 regarding the PSSAR form

2 New DCII Account Checklist

Following is a quick reference checklist to help prospective DCII Agency Administrators and Users complete the required steps to obtain a DCII account. This document includes detailed instructions for the creation of a new DCII Agency Administrator account as well as requirements for User accounts.

For ALL Accounts on DCII:

- Meet eligibility requirements:
  - The minimum requirement for DCII access is a completed, fully adjudicated single scope background investigation (SSBI) resulting in at least a Secret eligibility determination.
- Complete the Personnel Security System Access Request (PSSAR) Form.
- Complete Cyber Security Awareness/Information Assurance training (2 options)[1]:
  - https://public.cyber.mil/training/cyber-awareness-challenge/
  - Security training course provided by the cleared service/company/agency
- Complete Annual security training provided by the cleared Service/company/agency
- Complete Personally Identifiable Information training (2 options)[1]:
  - https://iatraining.disa.mil/eta/piiv2/launchPage.htm
  - http://www.cdse.edu/catalog/elearning/DS-IF101.html (if you have a STEPP account)
  - Approved existing corporate PII training courses

Once all elements in the list are completed, refer to the instructions that follow to submit your documentation.

[1] This information can be found on the PSA Website under the DCII tab.

3 How Do I Obtain a DCII Account?

3.1 DoD Agencies and Military

DCII Agency Administrators: To obtain a new DCII account required to perform your job duties on behalf of a DoD Agency or the military (applicants may be active duty military, civilians or government-sponsored contractors) please submit the following to the DCSA Contact Center:

- A DCII PSSAR form completed, signed, and submitted for each applicant. The signatories need to be your Nominating Official or delegate (GS-14 grade or military branch equivalent), your Security Officer, and the applicant (you). The PSSAR section that follows provides instructions for completing the form as well as a link to download the PSSAR.
- A copy of your certificates of completion for both the Cyber Security Awareness Challenge and Personally Identifiable Information courses (see links above). These must have been completed within the past year.
- The Rules of Behavior (ROB) document for DCII signed by the applicant indicating acknowledgment of roles and responsibilities. A copy of the ROB may be found on the DCSA PSA DCII website under the "DCII Resources -> Access Request". section.

After completing the PSSAR and gathering all necessary training certificates, see the **Submitting the PSSAR Form** section of this document. Review the **Most Common Reasons for PSSAR Rejection/Disapproval** section below to make sure your documents are correct prior to submitting.

DCII Agency Users: To obtain a new DCII account required to perform your job duties on behalf of an Agency, contact your agency's DCII Agency Administrator. The DCII Agency Administrator will process your request and will require the following documentation:

- A PSSAR form must be completed, signed, and submitted. The signatories need to be those of your agency Director (GS-14 grade or military branch equivalent), your Security Officer, and the applicant (you). The PSSAR section that follows provides instructions for completing the form as well as a link to download the PSSAR.
- A copy of your certificates of completion for both the Cyber Security Awareness Challenge and Personally Identifiable Information courses. These must have been completed within the past year.

3.2 Non-DoD Government Agencies

DCII Agency Administrators: To obtain a new DCII account required to perform your job duties on behalf of a Non-DoD Agency (applicants may be civilians or government-sponsored contractors), you will need to submit the following items:

- A PSSAR form completed, signed, and submitted. The signatories should include your Agency's Director or delegate (GS-14 grade or military branch equivalent), your Security Officer, and the applicant (you). The PSSAR section that follows provides instructions for completing the form as well as a link to download the PSSAR.
- Proof of your security clearance (e.g., CVS). A Single Scope Background Investigation (SSBI) with Secret eligibility is the minimum level required.
- A copy of your certificates of completion for both the Cyber Security Awareness Challenge and Personally Identifiable Information courses. These must have been completed within the past year.
- The Rules of Behavior (ROB) document for DCII system must be signed by each Agency Administrator indicating acknowledgment of roles and responsibilities. A copy of the ROB may be found on DCSA PSA DCII website under the "DCII Resources -> Access Request". section.

After completing the PSSAR and gathering all necessary training certificates, see the S**ubmitting the PSSAR Form** section of this document. Review the **Most Common Reasons for PSSAR Rejection/Disapproval** section below to make sure your documents are correct prior to submitting.

DCII Agency Users: To obtain a new DCII account required to perform your job duties on behalf of a Non-DoD Agency, contact your agency's DCII Agency Administrator. The DCII Agency Administrator will process your request and will require the following documentation:

- A PSSAR form must be completed, signed, and submitted. The signatories should include your Agency's Director or delegate (GS-14 grade or military branch equivalent), your Security Officer, and the applicant (you). The PSSAR section that follows provides instructions for completing the form as well as a link to download the PSSAR.
- A copy of your certificates of completion for both the Cyber Security Awareness Challenge and Personally Identifiable Information courses. These must have been completed within the past year.

4 DCII Account Policies

4.1 Account Activity

- **Active DCII Account**:

  An active DCII account is one that has been logged into in the past **30** days.

- **Inactive DCII Account**:

  An inactive DCII account is an account that has not been logged into in the past **30** days. If a DCII account continues to be inactive for **30-45** days, the account will be removed, and new documentation will need to be submitted prior to getting the account reactivated.

- **Deleted Inactive DCII Accounts**:

  DCII accounts that have not been logged into for longer than **45** days will be deleted per CYBERCOM TASKORD (13-0641). If a DCII account is needed after it has been deleted due to inactivity, a new account will have to be established following the aforementioned request procedures.

4.2 Violations / Misuse of DCII Accounts

By using the DCII application, all Administrators and Users are consenting to the application terms of use and agree to maintain compliance with the Privacy Act of 1974 and all applicable DCII rules and regulations, including the DCII Rules of Behavior.

Misuse of DCII will result in **termination** of the offender's DCII account and exclude culpable companies or persons from future access to DCII.

Misuses of DCII include, but are not limited to:

- Sharing usernames, passwords, CAC or PIV cards and/or associated PIN numbers to access the system,
- Allowing non-cleared individuals to access the system
- Leaving the DCII application unsecured while logged into it
- Allowing personnel to view data on the DCII screen who do not have the proper authorization
- Providing printouts of DCII data to personnel who do not have the proper authorization
- Querying the DCII application for information you have *no need to know in order to conduct your official duties*

5 Personnel Security System Access Request (PSSAR) Form

The PSSAR form must be completed for all new DCII accounts, modifications to existing DCII accounts, or deactivations of DCII accounts.

These quick tips are targeted for DCII account applicants to assist in correctly completing the form and speed application processing.

Part 1

This section collects applicants' personal information. Complete boxes 1-13. Items to pay particular attention to are:

- **Organization (2)** – The Agency requesting access to DCII. If you are a Service member or Government civilian, fill in your Service and unit information.
- **Official e-mail address (7)** – Use your official work address, do not enter personal email addresses (e.g., Google and Yahoo accounts are not appropriate for official business.)
- **Social Security Number (11)** – Do not leave blank. All Personal Identifiable Information (PII) is protected when encrypting the PSSAR form via email to the DCSA Contact Center. **To send sensitive information via email,** follow the instructions for establishing encryption capability with the DCSA Contact Center to ensure your privacy is protected: Contact Center Email Encryption.
- **Designation of Person (13)** – If the company listed in Box 2 is a DoD Contractor, select that option. If a Non-DoD Contractor, select that option. Do not select DoD Military or DoD Civilian unless you identified a DoD Organization as your employer in Box 2.

Part 2

List the date when **training** was completed and provide certificates of completion to the DCSA Contact Center or your Agency Administrator, as appropriate. If you have not taken the training yet, links to training references can be found on the PSA website. The training can be completed within 2-3 hours.

Part 3

The PSSAR form is also used to request access to other PSA applications. **Box 17** is the only section of Part 3 that needs to be completed for DCII access.

- **Agency Code or Agency Acronym** – These are DCII created codes. The agency code or acronym can be obtained from the current DCII Agency Administrator or Nominating Official. If you are unable to locate your agency code or acronym, please send a digitally signed email to the DCSA Contact Center requesting this information. Allow 1 to 2 business days for a response.
  - The Agency Code is a 2 to 3 digit code and the Acronym is 3 to 5 alphanumeric code.
- Select desired role or permissions by clicking the appropriate box. You will be limited by the permissions granted to your agency. An accreditation code is required for File Demand permissions.

Part 4 – Signature Required!

It is very important to fully understand the account policies, security policies and all applicable DoD regulations and U.S. Laws as you are agreeing to comply with them when you sign.

- Applicant's Signature (27) – Account Applicant must sign in this box.

Part 5 – Signature Required!

This section should be completed by the Nominating Official (GS-14 grade or military branch equivalent). This individual is the person who authorizes your access to the application and cannot be the same as the Applicant unless yours is a single person facility. Before signing, the Nominating Official should carefully read the certification.

- It is critical that the Nominating Official complete the **Statement of Duties**. The Statement of Duties should be entered following the words "These duties include:" in Part 5. The statement of duties must sufficiently justify the request for access to the DCII application; otherwise the PSSAR form will be rejected.

Part 6 – Signature Required!

Part 6 provides confirmation that the user meets the security requirements for the application. The Validating Official provides the final signature for the form and must be provided by the requesting Agency unless it is a single person facility, in which case this part will be completed by the DCSA Contact Center.

6 More PSSAR Tips

Be sure to put your Last Name, First Name, Middle Initial (or NMN) at the top of pages 1 and 2.

DCII Permissions Descriptions:

NOTE: Permissions granted to a User on the DCII system are limited to the permissions granted to the associated agency. If a new permission is requested that is not provided with the agency account, the PSSAR form will be rejected.

- **Query (Search):** Ability to search for person records in the DCII system.
- **Add:** Ability to add person records and investigation files to the DCII system. Investigation files can only be added to person records the Users' agency has entered.
- **Delete:** Ability to remove person records and investigation files from the DCII system. Users can only delete records that are were entered by their agency.
- **Update/Edit:** Ability to update the person record information within DCII for record
- **File Demand:** Grants the User the ability to request investigation files from the agency that performed the investigations. An agency accreditation code for the Users' affiliated agency is required for this permission. If you don't know what your accreditation code is, contact your Agency Administrator or send a digitally signed email request to the DCSA Contact Center.
- **File Demand Print:** Grants the User the ability to produce a report listing all File Demands made by the agency with which the User is associated. An agency accreditation code for the Users' affiliated agency is required for this permission. If you don't know what your accreditation code is, contact your Agency Administrator or send a digitally signed email request to the DCSA Contact Center.

DCII Role Descriptions:

- **Agency User:** Those that will be performing the basic functionality on the DCII system. Examples: Adding, deleting and/or updating person records and investigations within DCII. Searching for investigative records and making file demands are responsibilities of the Agency User.
- **Agency Administrator:** Responsible for creating, deleting and maintaining Agency User accounts.
- **Executive Administrator and Root Administrator:** These roles are for DCII INTERNAL USE ONLY; do not select them when requesting an account.

7 Most Common Reasons for PSSAR Rejection/Disapproval

Avoiding these pitfalls will enhance the processing/approval timeline of your PSSAR submission, as long as account/access eligibility requirements are met.

1. **Missing Training Certificates** –
   Cyber Security Awareness/Information Assurance and Personally Identifiable Information (PII) courses are required annually. If you have not taken the course within the past year, you will need to update your training certification before submitting the form. All certificates must accompany the PSSAR form. See below for more instructions about submitting training certificates.
2. **No Statement of Duties in Nominating Official's Section** –
   Duties which justify the request for access to the application MUST be listed.
3. **Missing Signatures** –
   All three required signatures (Parts 4, 5, and 6) **must** be provided on the PSSAR form.
4. **Obsolete PSSAR Form Submitted** –
   The current PSSAR is available at the following link. Do not submit the Sample PSSAR for DCII, JPAS, or SWFT, as they will not be accepted or processed.
5. **Applicant Not Eligible Due to Lack of Appropriate Security Clearance** –
   At a minimum, a completed and favorably adjudicated single scope background investigation (SSBI) with at least a Secret eligibility is required for a DCII account. Applicants should not submit a PSSAR form if they don't meet these criteria.
6. **Agency Code or Agency Acronym Not Listed in DCII** –
   The Agency code or Agency Acronym listed on the PSSAR could not be found on the DCII system. A correct Agency code or Acronym must be provided to set up new accounts on DCII. Contact the DCSA Contact Center to request either the code or the acronym.
7. **SSN Not Located in JPAS** –
   The social security number (SSN) on the PSSAR was not located in JPAS. This would indicate either the SSN was entered incorrectly on the PSSAR or the applicant does not meet the minimum DCII account eligibility/access requirements and therefore does not have a record in JPAS. Non-DoD agency applicants also might not have a record in JPAS so access eligibility for them would need to be confirmed by other methods (e.g., OPM CVS).
8. **Requesting both an Agency User and Agency Administrator account on same PSSAR form –**
   DCII Agency Administrators: Only select 'Agency Administrator' from **Box 17.**
   DCII Agency Users: Applicants can choose one or more of the following permissions for a DCII Agency User account: Add, Delete, Update, Query (Search), File Demand Print, or File Demand (Accreditation Code required) from **Box 17**.
   Do not select both 'Agency Administrator' and Agency User accounts on a single PSSAR. Agency Users should provide a separate PSSAR to their Agency Administrator for a User account. *Please do not submit this PSSAR form to the DCII Contact Center for processing. The Contact Center does not create User accounts.*

7.1 Submitting the PSSAR Form and Training Certificates

Completed PSSAR forms and training certificates for Agency Administrators applicants should be submitted to the DCSA Contact Center. Agency User applicants should submit their PSSAR forms and training certificates to their Agency Administrators.

DCSA Contact Center Email: dcsa.ncr.nbis.mbx.contact-center@mail.mil

NOTE: To send sensitive information via email, such as **Personal Identifiable Information** (PII), please follow the instructions for establishing encryption capability with the DCSA Contact Center to ensure your privacy is protected: Contact Center Email Encryption.

7.2 Sample DCII PSSAR Form

A sample PSSAR form follows to assist DCII account applicants. **DO NOT** submit a filled in version of the sample, as it will not be accepted.

Download a blank application form from the PSA website (Defense Counterintelligence and Security Agency > Information Systems > Defense Central Index of Investigations (DCII) (dcsa.mil) under ‘Access Request’.