# Defense Manpower Data Center

DISS Account Request Procedures
Document v1.1

Defense Information System for Security (DISS)
October 2017

# Table of Contents

| REVISION HISTORY | | | |
|---|---|---|---|
| Date | Version | Change Description | Author |
| 12/29/2016 | 1.0 | Initial Draft | Xcelerate Solutions |
| 10/31/2017 | 1.1 | Update new link for Cyber Awareness Training | DISS PMO |
| | | | |

# 1.0 New DISS Account Checklist

Following is a quick reference checklist to assist prospective DISS Portal users in completing the required steps for a DISS Portal account. All documentation is required regardless of whether you are requesting a new account, or you are submitting for an account after having a previous account deleted due to inactivity.

*Note*: To access the DD Form 2962, Personnel Security System Access Request (PSSAR), click on the following link: DISS PSSAR

Please read the entire procedure to ensure all requirements are met before submitting your request.

- ☐ Meet clearance requirements:
  The minimum requirement for DISS Portal access is Interim Secret eligibility with a valid open investigation.
- ☐ An Active owning and/or servicing Security Management Office (SMO), for Industry this means an active facility clearance (see section 2.3.2).
- ☐ Obtain an active PKI Certificate on a smartcard (CAC, PIV card, ECA PKI Certificate or other approved DOD PKI on a smartcard/token) prior to getting a DISS Portal account [1,2]

- ☐ **Take Cyber Security Awareness/Information Assurance course (2 options)[2] and include your course completion certificate:**
  **1. https://iatraining.disa.mil/eta/disa_cac2018/launchPage.htm**
  **2. Annual security training provided by the cleared service/company/agency**
- ☐ **Take Personally Identifiable Information (PII) course (2 options)[2] and include your course completion certificate:**
  **1. http://iatraining.disa.mil/eta/piiv2/launchPage.htm          or,**
  **2. http://www.cdse.edu/catalog/elearning/DS-IF101.html (need STEPP account)**
- ☐ Complete DD Form 2962, PSSAR
- ☐ Submit Letter of Appointment (LOA), if applicable. A LOA is required for ALL Hierarchy Managers

*\* Note: Industry users subsequently being provisioned by the responsible Hierarchy/Account Managers may submit company approved PII training certificates.*

**Once all elements in the list are completed**, please refer to the instructions below to submit your documentation to the appropriate DISS Portal Hierarchy Manager or Account Manager. **DO NOT** submit requests to the DMDC Contact Center unless you are requesting an Industry Primary Hierarchy Manager account. The OSD Defense Agencies and Military Services must go through their Hierarchy Manager or

---

[1] Due to identity validation processes, PKI issuance can take some time. It is highly recommended to have your PKI hardware & certificates on hand before requesting an account as the account activity timer starts from when the account is created **not** from when the PKI is registered.
[2] See section 3.4 of our Account Management Policy for background and requirements for mandatory trainings. Please submit the actual course completion certificates - not memos, emails or automated logs.

Account Manager. Hierarchy/Account Managers are responsible for managing the accounts, keeping the PSSAR form, and training certificates.  These items will be asked for during an audit or incident.

# 2.0   How Do I Obtain a DISS Account?

## 2.1 Introduction

There are two roles within the system that can create user accounts, the Hierarchy Manager and the Account Manager. The Hierarchy Manager is the head of the SMO, and manages the organizational structure of the Security Management Office. The Hierarchy Manager must be initially provisioned by the Help Desk for a SMO, once a SMO has a Hierarchy Manager, they can assign any additional Hierarchy Managers to the SMO. The Account Manager manages the Security Officers and users within their hierarchy by creating user profiles and assign roles and permissions. Account Managers are provisioned by the SMO's Hierarchy Manager. For a full list of Roles and Permissions within the system, please refer to Appendix A in the DISS Account Management Policy.



*Figure 1- DISS Portal Role Hierarchy*

## 2.2 Military Services and OSD Defense Agencies

To obtain a new DISS account required to perform your job duties on behalf of a military service/OSD Defense Agency (applicants may be active duty military, civilians or contractors), contact an established DISS Portal Hierarchy Manager or Account Manager within your military service/OSD Defense Agency. If you do not know whom to contact, please refer to the DISS Point of Contact (POC) Listing on the DMDC DISS User website to locate a DISS PMO for your military service/OSD Defense Agency. To request an account, your DISS Account Manager will need a DISS PSSAR form must be completed, signed, and submitted.  The signatures need to be your Commanding Officer, your Security Officer, and the applicant. A copy of your certificates of completion for both the Cyber Security Awareness Challenge/Security training as well as one of the PII courses must be submitted with your PSSAR.

*Note*: If a new Hierarchy Manager is required, also submit a LOA on your military service/OSD Defense Agency letterhead indicating who the account is for and the specific job duties that require DISS access to your Hierarchy Manager. Your Branch/Agency Director or delegate must sign the letter. Delegates must be GS-14 grade (or military branch/Agency equivalent) or higher.

## 2.3 Industry

### 2.3.1 Hierarchy Managers:

If a Hierarchy Manager already exists at your company, submit all of the items in the Users section below, PLUS a LOA, to your existing Hierarchy Manager. Requests for additional Hierarchy Managers should **not** be submitted to the DMDC Contact Center.

If there are **no** existing Hierarchy Managers for your company, follow the process below and request to be the primary Hierarchy Manager for your company. The DMDC Contact Center will create your account. To request an account, you will need to submit the following items:

- A LOA on your company's letterhead naming the applicant as the company's primary DISS Hierarchy Manager.  A Key Management Personnel (KMP) listed in Industrial Security Facilities Database (ISFD) must sign the letter.
- A PSSAR form must be completed, signed, and submitted.  The signatures need to be those of your KMP, your Security Officer, and the applicant.
- A copy of your certificates of completion for both the Cyber Security Awareness Challenge/Security training as well as one of the government approved Personally Identifiable Information courses must be submitted with your PSSAR.
- If you are a new Hierarchy Manager or KMP at a cleared company, you will need to have both a facility clearance as well as a proper servicing relationship.  For instructions on obtaining a facility clearance please see the checklist for a New Facility Clearance.

*Note*: A DISS user can have multiple facilities under their DISS account. However, a user can only request 1 facility per PSSAR, as the KMP of the facility needs to sign it. Typically the KMP is not the same for all the facilities.

After completing a PSSAR, certificates of training completion, and the LOA, please submit all to the DMDC Contact Center, as described in the Submitting the PSSAR Form section 2.2 of this document. Once the account has been created, the DMDC Contact Center will contact you with your initial log-in credentials.

### 2.3.2 Users:

To obtain a new DISS account required to perform your job duties on behalf of an Industry company, you will need to contact your company's DISS Hierarchy Manager or Account Manager. Your DISS Hierarchy Manager or Account Manager will process your request. To request an account, your DISS Hierarchy Manager or Account Manager will need:

- A PSSAR form must be completed, signed, and submitted.  The signatures need to be those of your KMP, your Security Officer, and the applicant.
- A copy of your certificates of completion for both the Cyber Security Awareness Challenge/Security training as well as one of the government or company approved Personally Identifiable Information courses must be submitted with your PSSAR.

## 2.4 Non-DOD Government Agencies

DISS accounts for non-DOD government agencies are issued by exception due to the lack of insight into non-DOD subjects' employment, security clearances, or oversight. If a non-DOD government agency requests a DISS account, the agency must have a National Industrial Security Program (NISP) agreement with the Department of Defense for industrial security services. In addition, the non-DOD government agency must provide formal justification for requesting a DISS account. This explanation will include the reasons why the agency cannot use the Office of Personnel Management's (OPM) Central Verification System (CVS) database to verify contract clearance information. Agencies that have existing agreements with the DOD for industrial security services are listed in the National Industrial Security Program Operating Manual (NISPOM), paragraph 1-103b, and do not include sub-agencies.

# 3.0  Deactivate/Delete a DISS Account

DISS accounts shall NOT be transferred between organizations/companies.  If a Hierarchy Manager, Account Manager, or user leaves an organization/company, the associated account in DISS must be deactivated by the owning organization/company.

To deactivate a DISS account, fill out a "deactivate" PSSAR to remove all DISS access and disable an existing account. Complete the following fields of the PSSAR form:

- Type of Request (select "deactivate")
- User ID Field, if known
- Date
- Box 1, Name of account holder
- Box 5, Official E-Mail Address (enter the email address of the Nominating Official so that DMDC Contact Center can communicate the completion of the request)
- Box 11, SSN of account holder
- Box 24, Nominating Official's Printed Name
- Box 25, Nominating Official's Title
- Box 26, Nominating Official's Telephone Number
- Box 27, Nominating Official's Signature
- Box 28, Nominating Official's Date

Hierarchy Managers or Account Managers should deactivate accounts of other Hierarchy Managers/Account Managers or other users within their Security management Office, according to the provisions of the DISS Account Management Policy.  In the event when an organization or company does not have a Hierarchy Manager or Account Manager to perform the deactivation of accounts, please

submit the deactivation request to the DMDC Contact Center by following the steps outlined in the DISS Account Management Policy section 4.3.

*Note*: LOA and Training Certificates are NOT required for deactivate account requests.

# 4.0  DISS Account Policies

## 4.1 Account Activity

- **Active DISS Account**:
An active DISS account is one that has been logged into in the past **30** days.

- **Inactive DISS Account**:
An inactive DISS account is an account that has not been logged into in the past **30** days. If a DISS account is inactive for **31-44** days, the DISS system will automatically lock the account. Only the company/agency Account Manager overseeing the user's account will be able to unlock the account.

- **Deleting Inactive DISS Accounts**:
DISS accounts that have not been logged into for longer than **45** days will be deleted per DOD Regulations (CYBERCOM TASKORD 13-0641).  If a DISS account is needed after it has been deleted due to inactivity, a new account will have to be established following the aforementioned request procedures to include all required documentation.

## 4.2 Violations/Misuse of DISS Accounts

By using the DISS application, users are consenting to the terms of use of the application and are agreeing to maintain compliance with the Privacy Act of 1974 and all applicable DISS rules and regulations, including the DISS Account Management Policy.

Misuse of DISS will result in **termination** of the offender's DISS account and exclude culpable companies or persons from future access to DISS. Additionally, offenders will have a misuse of technology incident recorded on their DISS record. Information concerning violations of DISS policies and may be referred to other federal agencies for consideration of administrative, civil, or criminal sanctions when circumstances warrant.

Common misuses of DISS include, but are not limited to:
- Sharing of username, password, CAC, or PIV cards and/or associated PIN numbers to access the system
- Allowing non-cleared individuals to access the system
- Leaving the DISS application unsecure while logged in
- Allowing others to view data on the DISS screen that do not have the proper authorization
- Printing or taking a screenshot of DISS data
- Querying the DISS application for high profile records
- Entering test or "dummy" SSNs into DISS

- Entering false or inaccurate information into the system
- Hierarchy/Account Managers are not authorized to manage their individual DISS accounts
- Querying the DISS application for information you have no need to know to conduct your official duties