Defense Counterintelligence and Security Agency

NBIS Account Management Policy Document v 1.2.1

National Background Investigation Services (NBIS)

April 2022

Contents

1.0 PURPOSE 3
2.0 BACKGROUND 4
3.0 ORGANIZATION ROLES AND RESPONSIBILITIES 5
3.1 NBIS Program Management Office 5
3.2 Defense Vetting Directorate Enterprise Business Support Office 5
3.3 NBIS System Liaison Support 5
3.4 NBIS Account Management 5
3.5 Mandatory Training Courses for NBIS Access 6
4.0 ACCOUNT LIFECYCLE 8
4.1 NBIS Account Requirements 8
4.1.1 Personnel Security System Access Request Form (DD Form 2962) 8
4.2 Account Transfer Between Agencies, Organizations, or Companies 8
4.3 Unexpected Loss of an Organization Manager, Workflow Manager, or User Manager 9
5.0 SECURITY 9
5.1 Security Clearance Requirement 9
5.2 System Data and the Privacy Act 9
5.3 Two-Factor Authentication and Password/PIN Management 9
5.4 Account Activity 10
5.5 Misuse of NBIS 10
6.0 ACRONYMS 11
Appendix A: User Role Matrix 12
Appendix B: End-User Quick Start Guide 14

1.0 PURPOSE

This policy outlines account management guidance for the National Background Investigation Services (NBIS) System. This policy is maintained by the NBIS Planning and Deployment Office (PDO) and shall be reviewed bi-annually.

This document is intended as a guide for end users of the system. It defines NBIS System and its intended uses, details the roles and responsibilities associated with the system, enumerates and describes the requirements to gain and maintain access, and also describes the key security requirements to which users must adhere and of which they must remain mindful as they use the system.

2.0 BACKGROUND

The Department of Defense (DoD) developed the information technology capabilities that contribute to NBIS to support federal background investigation processes pursuant to Executive Order 13467, as amended, and Section 925 of the National Defense Authorization Act (NDAA) for FY2018. NBIS integrates information technology capabilities to conduct background investigations activities including: investigations and determinations of eligibility for access to classified national security information, and for access to special access programs; suitability for federal employment; fitness of contractor personnel to perform work for or on behalf of the U.S. Government; and Homeland Security Presidential Directive (HSPD)-12 determinations for Personal Identity Verification (PIV) credentials to gain logical or physical access to government facilities and systems. NBIS also supports submissions of adverse personnel information; verification of investigation and adjudicative history and status; continuous evaluation; and insider threat detection, prevention, and mitigation activities.

NBIS is the DOD System of Record for personnel security and will replace the Defense Information System for Security (DISS), which itself was designed to replace the Joint Personnel Adjudication System (JPAS). Users within the federal government and private industry will use NBIS to conduct comprehensive personnel security management for all cleared personnel.

3.0 ORGANIZATION ROLES AND RESPONSIBILITIES

3.1 NBIS Program Management Office

The PDO is responsible for the formulation of NBIS account management policy, enforcement of that policy, and the account administration for the primary NBIS User Managers for the Military Services; DoD; federal agencies; contractors; and, state, local, and tribal governments.

3.2 Defense Vetting Directorate Enterprise Business Support Office

The DVD PDO is responsible for the formulation of system capabilities and requirements for NBIS derived from stakeholder engagement. New capabilities are researched, vetted, and piloted through the DVD PDO. New requirements or changes to existing requirements are evaluated and prioritized through a governance process.

3.3 NBIS System Liaison Support

NBIS Technical Support is defined as customer support needed to resolve issues concerning user browser configuration, NBIS accessibility via the Internet, and system malfunctions. Users may be required to contact their local area communications or network support for issue resolution.

The DCSA Consolidated Knowledge Center provides technical support to all users but only provides Account Management support to the primary NBIS User Managers. Issues or concerns that require the attention of the NBIS Program Manager should be submitted to the DCSA Consolidated Knowledge Center. For additional information, contact the Knowledge Center at (724) 794-5612, ext. 4600.

3.4 NBIS Account Management

Organizational administration of NBIS is primarily divided into three roles. The Organization Manager role allows the user to create a robust agency hierarchy, stretching down as many levels as required. The Organization Manager can be a user at any level of the hierarchy, but the permission only grants them the ability to build a structure from that point in the hierarchy and down, never back up. The User Manager role allows the user to create additional users, to assign them to their own organization or to any organization beneath their own in the hierarchy. The User Manager role is responsible for ensuring proper paperwork is submitted prior to creating the account and for associating that paperwork with the account in NBIS. Finally, the Workflow Manager role establishes the paths that work will take as part of an agency's business process. In some cases, work will remain internal to a single organizational element while in other scenarios, work may traverse multiple organizational elements. The Workflow Manager can neither create users nor create organizations but can ensure they work together seamlessly in how work is routed.

Note that while the functions have been separated into multiple roles, a user can have multiple roles as well. The flexibility of the NBIS role management system should allow for any number of possible user configurations and allow an agency to place a myriad of controls on who has access to which activities.

In addition to the roles listed above, two additional roles have been provided to enable a single organizational element to better manage itself. A Team Structure Manager is able to establish a hierarchy that is internal to a single organizational element. This is often used to group a single agency's users logically into teams and branches. Functionally this role operates in much the same manner as an Organization Manager; however, the hierarchy is limited to a single organization and

that hierarchy is not visible to external components. The Team User Manager is the second role provided for this purpose. This role is useful for moving users between various teams and configuring a user's capabilities and assignment preferences. A Team User Manager cannot create a new user account but can significantly affect the permissions of one that is already established.

The intent of NBIS is for the Onboarding Team to establish the first user in an agency and empower that user with the tools and knowledge they need in order to create subordinate units and users. This version of a train the trainer model will ensure maximum product delivery speed by treating each new user with an Org Manager, User Manager, or Workflow Manager role as a force multiplier. Agencies will not have to submit tickets for changes to structures or permissions, and these responsibilities can be delegated as far down the chain as an agency desires.

Organization Managers and User Managers may establish organizational policies to supplement this document; however, those policies may not conflict with this policy document or guidance from the PDO.

The users with User Manager Role shall be required to provide account management support for users as set forth in this policy. User Managers shall follow any additional guidelines set by their organization for the courtesy management of another organization's account while adhering to any guidance provided by the PDO. A User Manager is not authorized to manage his or her individual NBIS account. Organization Managers shall create all offices necessary to accurately represent their organization and provide support for any office within their own hierarchy, including Multiple Facility Organizations or corporate family. User Managers may only create user accounts for individuals within their own hierarchy.

3.5 Mandatory Training Courses for NBIS Access

The Personnel Security System Access Request (PSSAR, DD Form 2962) includes an acknowledgement that the user has "completed the necessary training with regards to Cyber Awareness and safe-guarding Personally Identifiable Information." The PSSAR specifically refers to the following courses required to receive an NBIS user account:

- Cyber Awareness Challenge/Information Assurance (IA) Security Training (two options available):
  - DoD Cyber Exchange's Cyber Awareness Challenge
  - Service, company, or agency approved cyber awareness/IA security training course
- Personally Identifiable Information (PII) Training (three options available):
  - DoD Cyber Exchange's Identifying and Safeguarding Personally Identifiable Information (PII) Training
  - CDSE's Identifying and Safeguarding Personally Identifiable Information (PII) Course (requires a STEPP account)
  - Service, company, or agency approved PII training course*

***Note**: Service, company, or agency approved cyber awareness, IA, and/or PII training course certificates may ONLY be used and submitted to an already established NBIS User Manager for new user account provisioning.*

All initial NBIS User Manager account requests submitted to DCSA require the new user to complete the DoD Cyber Exchange, or Center for Development of Security Excellence (CDSE) provided courses, as specified in section 3.5.

Appropriate training certificates shall be completed and uploaded directly into NBIS.

The following policies place the impetus for maintaining confidentiality, integrity, and availability for NBIS:

- DoD Instruction 8500.01 Cybersecurity and the Federal Information Security Modernization Act of 2014: Stipulates that all employees and contractors involved with the management, use or operation of DoD information systems must receive annual information assurance training and training on the use of personally identifiable information.
- DoD 5220.22-M, May 18, 2016: Annual refresher training is required to review security principles and responsibilities and to emphasize new security policies and practices developed from the preceding year.
- ISL 2012-03, May 14, 2012: FSO Training (NISPOM 3-102) National Industrial Security Program Operating Manual (NISPOM) paragraph 3- 102 requires contractors to ensure Facility Security Officers (FSOs) and other contractor personnel performing security duties complete security training considered appropriate by the Cognizant Security Agency (CSA).
- NISPOM 1-201, May 28, 2014: Facility Security Officer – The FSO, or those otherwise performing security duties, shall complete security training as specified in Chapter 3 and as deemed appropriate by the CSA.

Note: All new or modified account requests (to include account re-creation after deletion due to inactivity) will need to include proof of completion for these courses in addition to the PSSAR. Please reference section 4.1.1 below on how to access the PSSAR.

DCSA will not maintain training certificates of completion beyond the new account request procedure. It is up to the individual/organization to maintain proof of annual training as DCSA may request it during a security incident or audit.

4.0 ACCOUNT LIFECYCLE

4.1 NBIS Account Requirements

Access to the NBIS application shall be granted only if necessary to complete an individual's job duties. In order to receive an NBIS account, a potential user must have, at minimum, a favorable eligibility determination of a T1 investigation. All user roles and permissions will be based upon a user's job requirements. NBIS access will be immediately suspended if a user's eligibility determination has changed to Denied, Revoked, Loss of Jurisdiction, or Action Pending.

Access to NBIS is authorized via means of company-issued or government-owned/approved equipment with the appropriate security controls in place. NBIS users may not access their accounts from personal or home computers or over unsecured wireless networks. Sharing user names and passwords or PKI-logon credentials are prohibited and will result in termination of the offender's NBIS account. Additionally, a misuse of technology incident will be recorded on the offender's NBIS record. If the offender is part of a contract, the offender's contracting office may be notified of the security incident.

4.1.1 Personnel Security System Access Request Form (DD Form 2962)

The Personnel Security System Access Request Form is used to collect information required to grant an account in the NBIS System, to formally document the account request, and to provide accountability for the account. PSSARs are also used to request account deletions and to make changes to user roles and permissions. The PSAAR should indicate the name of the applicant and the specific job duties that require NBIS access. Access the "Personnel Security System Access Request (PSSAR) Defense Counterintelligence and Security Agency (DCSA) Volume 2 (DD2962v2)" form on the Washington Headquarters Service website at the following link: https://www.esd.whs.mil/Directives/forms/dd2500_2999/.

PSSARs shall be completed and filed for all users of the system. PSSARs shall have the signature of the individual requesting an account, the signature of the nominating official, and signature of the validating official before account access is granted. The nominating official CANNOT be the same as the requestor.

4.2 Account Transfer between Agencies, Organizations, or Companies

NBIS accounts will not be transferred between organizations. If a user leaves an organization, the user's organization associated persona in NBIS must be disabled by the owning organization. If NBIS access is required at the new organization, a new NBIS account will be created by the gaining organization.

4.3 Unexpected Loss of an Organization Manager, Workflow Manager, or User Manager

An inability to manage an account may occur for a variety of reasons, e.g., job change, death, major illness, etc. Establishing contingencies for these potential losses is the responsibility of each Agency and organization. Each Agency and organization should consider nominating both a primary and alternate point of contact for these roles.

5.0 SECURITY

NBIS was designed from the ground up as a secure system. One of its foundational cornerstones is protection of personally identifiable information and other sensitive data. While the system has many capabilities that will be transparent to end users, users of the system must exercise due care in the protection of information entered into or retrieved from NBIS. End users should refer, agree, and adhere to all security advisements displayed in security banners within the system. What follows are key security requirements to which users should ensure compliance, outlined here in simplified plain language. Users should keep in mind that the topics below are not all inclusive and should refer to system security banners displayed within NBIS and other relevant and appropriate security policies.

5.1 Security Clearance Requirement

At a minimum, NBIS users must possess a favorably adjudicated Tier 1 investigation. Higher level investigations may be required consistent with the user's position description requirements as determined by the Position Designation Tool.

5.2 System Data and the Privacy Act

NBIS is intended for use by security managers/security officers to update other users with pertinent personnel security clearance access information in order to ensure the reciprocal acceptance of clearances throughout the DOD. It also contains adjudicative information, incident reports, investigative data, and other sensitive information, protected and controlled by role-based access. Additionally, the contents of the NBIS system must be protected in accordance with appropriate policies governing such information, which may also be subject to the Privacy Act of 1974. Under the Privacy Act of 1974, personnel information retrieved through NBIS must be safeguarded. Disclosure of information is in IAW instructions as noted on security banners associated with the NBIS system. Above all, users must remember that, while NBIS is a highly secure system, proper training and adherence to policies concerning the protection of sensitive data and PII is an essential and foundational requirement for responsible use by all personnel.

5.3 Two-Factor Authentication and Password/PIN Management

Access to NBIS is controlled through the protections afforded by Public Key Infrastructure (PKI) compliance and two-factor authentication. This means that users will need a FIPS 201, PKI compliant CAC or smart card. It is a violation of DoD regulations to share authentication mechanisms including any username/password or any approved PKI Certificate. NBIS accounts are only provisioned for authorized individuals, as a result, there are no company, office, or shared accounts. Only the authorized account holder is permitted to view, access, or use the NBIS account via a subject's individually issued PKI credential

The system will lock a user ID after three consecutive failed attempts at the self-registration screen. User accounts can be unlocked only by the associated NBIS User Manager.

The NBIS PMO and Consolidated Knowledge Center can force password changes for Hierarchy

Managers within NBIS. NBIS User Managers can force password changes within NBIS for their organization's users.

PINs are alpha numeric codes associated with your PKI credentials and are managed differently depending on the specific type of credential used:

- For a DoD CAC, you have 3 attempts to enter a correct PIN. If you fail on the 3rd attempt, your credentials will be locked. To unlock your credentials, you will need to visit a DEERS/RAPIDS station to unlock and subsequently use.
- For a federal PIV, contact the issuer of the PIV for their reset policies.
- For ECA and other DoD approved PKI credentials, this process can vary between issuers.

Note: some issuers do not conduct a PIN/Password reset and will require the purchase of a separate credential.

5.4 Account Activity

As an additional security measure, users should be aware that if an NBIS account is inactive (i.e., not accessed for more than 30 days), the system shall automatically lock the account. The NBIS User Manager will be able to unlock the account, unless the account exceeds 45 days of inactivity. NBIS accounts that have not been logged into for longer than 45 days are deleted per DoD Regulations (CYBERCOM TASKORD 13-0641).

5.5 Misuse of NBIS

Misuses of NBIS 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 NBIS application unsecure while logged in.
- Allowing others to view data on the NBIS screen that do not have the proper authorization.
- Printing or taking a screenshot of NBIS data.
- Querying the NBIS application for 'celebrity' records.
- Entering test or "dummy" SSNs into NBIS.
- Entering false or inaccurate information into the system.
- Querying the NBIS application for information you have no need to know to conduct your official duties.
- Org Managers are not authorized to manage their individual NBIS accounts.

DCSA as the System Manager (SM), Program Manager (PM), and Authorizing Official (AO), has the responsibility and ability to make determinations regarding system access, especially when a misuse of the system has occurred that may require an adjudicative determination. This Responsibility and authorization for DCSA to make risk-based authorization decisions is stated in the DoDI 8500.01 Enclosure 3: Procedures, Section 2: Risk Management, (3)(b), as well as Enclosure 3: Procedures, Section 16: AO, (a)(b).

6.0 ACRONYMS

AO	Authorizing Official
CSA	Cognizant Security Agency
DoD	Department of Defense
DVD	Defense Vetting Directorate
PDO	Enterprise Business Support Office
FSO	Facility Security Officer(s)
KMP	Key Management Personnel
NBIS	National Background Investigation Services
NDAA	National Defense Authorization Act
NISPOM	National Industrial Security Program Operating Manual
PDT	Position Designation Tool
PII	Personally Identifiable Information
PIV	Personal Identity Verification
PKI	Public Key Infrastructure
PM	Program Manager
PMO	Program Management Office
PSSAR	Personnel Security System Access Request
SM	System Manager
SMO	Security Management Office

Appendix A: User Role Matrix

The following table reflects the current roles and responsibilities built within the NBIS System. The table documents how these roles align to the roles listed on the Personnel Security System Access Request (PSSAR) form and provides guidance on a few additional roles that are solely listed on the PSSAR form. Please use this table for guidance when completing the PSSAR form. If an NBIS System User Role is needed that is not listed on the PSSAR, use the "Other" box and "elevated permissions" form field to specify the required NBIS System User Roles.

NBIS System User Role Matrix

NBIS System User Role	PSSAR – 19a Role	Responsibility
Authorizer	Authorizer (Government Only)	An Organization User who reviews entire cases, completes financial details, edits certain order form details, and decides whether to approve, reject, or hold cases.
Initiator	Initiator	An Organization User who initiates the Subject/employee, selects form(s) to be completed by the Subject, completes Agency Usage Block (AUB), contacts Subjects/employees to inform them that they should complete the investigation form(s) using eApp, requests an Authentication reset, and cancels/un-cancels requests.
NBIS Financial Manager	NBIS Financial Manager	NBIS system manager for NBIS financial setup. Creates IPAC, IPAC Exemption BETC, and TAS billing codes. Can also manage SON/SOI and SON/IPAC for all orgs. Additional information can be found about financial codes at: http://nbib.opm.gov/hr-security-personnel/requesting-opm-personnel-investigations/
Notification Manager	Notification Manager	Responsible for creating, customizing, and managing criteria for automatic alerts that can be used throughout the lifecycle of a case.
Order Form Template Manager	Order Template Manager	Responsible for building, managing, and distributing the Order Form Templates for an Organization.
Org Assignment Manager	Business Process Manager	Responsible for setting an Organization's priorities for work assignments to enable the automatic routing of tasks.

NBIS System User Role	PSSAR – 19a Role	Responsibility
Org Manager	Org Manager	Responsible for creating an Organization's hierarchy and assigning associated roles for each hierarchy element.
Org Workload Manager	Workload Manager	Responsible for managing user capabilities and skillsets in an Organization, including manually assigning and reassigning cases to users.
Reviewer	Reviewer	An Organization User who reviews the submitted standard form (SF8X) for accuracy and completeness and determines whether the form is sufficient to move the request for investigation forward (i.e., makes go / no-go decision).
Task Reassignment		An Organization User who has permission to reassign their own workload to other people.
Team Structure Manager	Internal Org Manager	Responsible for creating and managing teams (i.e., internal structures within an Organization's hierarchy).
Team Workload Manager	Internal User Manager	Responsible for overseeing the work within the Teams previously established by the Team Structure Manager.
User Manager	User Manager	Responsible for establishing roles and permissions for individuals within an Organization, Sub-Organization(s), and Team(s).
Workflow Manager	Workflow Manager	Responsible for determining the routing of new case initiations through the review, authorize, and investigation processes.
	System Manager	This role is currently not available for agency assignment.
	Financial Manager	This role is currently not available for agency assignment.
	Point of Contact	This role is currently not available for agency assignment.
	Other	Covers future roles that are currently not listed on the PSSAR form. Select this option on the PSSAR and insert the role requested .

Appendix B: End-User Quick Start Guide

Step 1: Obtain an active PKI compliant smartcard (CAC, PIV card, ECA PKI Certificate or other approved DoD PKI on a smartcard/token) prior to getting an NBIS account.

Step 2: Meet the minimum personnel security requirements for access to NBIS.

Step 3: Work with your SMO or organization's leadership to determine your appropriate role(s) and responsibilities within NBIS. Refer to Appendix A for a list of NBIS roles. Note, users may have one or more NBIS roles required to accomplish their assigned duties. Refer also to the NBIS Account Management section for more information about establishing accounts.

Step 4: Your organization's NBIS User Manager will work with you to complete a Personnel Security System Access Request Form (DD Form 2962).

Step 5: Complete all mandatory training as a prerequisite of NBIS access.

Step 6: Review and comply with appropriate security requirements.