Do Not Pay
User Enrollment Guide
for PIV, CAC & LincPass
Card Users

August 2019
**Table of Contents**

About This Enrollment Guide ................................................................. 3

I. DNP OVERVIEW ................................................................................. 3

   DNP Business Center Components: ................................................ 4

      Web-based Portal ........................................................................... 4

      Data Analytics ................................................................................ 4

      Agency Support ............................................................................. 4

PIV Onboarding Process Overview .................................................. 5

II. COMPLETING FORMS ..................................................................... 6

   Senior Agency Outreach Liaison Sends User Enrollment Form .......... 6

   Access Group Administrator (AGA) Completes and Signs the User Enrollment Form .... 6

III. EMAILS .............................................................................................. 7

   DNP Rules of Behavior Email .......................................................... 7

   IBM Security Identity Manager (ISIM) Email .................................... 8

IV. GAINING ACCESS TO THE PORTAL USING A PIV CARD ............. 19

   Linking Your PIV Credentials .......................................................... 19

V. LOGGING INTO THE DNP PORTAL .................................................. 22

   Open Your Internet Browser ............................................................ 22

   Fiscal Service Enterprise Single Sign On .......................................... 22

   DNP Portal: Homepage .................................................................... 24

VI. USER GUIDE .................................................................................... 26

VII. TROUBLESHOOTING ................................................................. 27

   Unable to Log into the DNP Portal ................................................... 27

   Issues on Downloading Text or Excel File with Existing Browser ...... 28

VIII. SYSTEM REQUIREMENTS .......................................................... 29

IX. FREQUENTLY ASKED QUESTIONS (FAQs) .................................... 30

X. GETTING HELP .................................................................................. 31
About This Enrollment Guide

This guide is intended for new users of the Do Not Pay Portal (the Portal) that use a Personal Identity Verification (PIV), Common Access Card (CAC), or LincPass Card. This guide illustrates the steps necessary to gain access to the Portal. The information in this reference guide has been divided into nine sections. Each section provides a brief description of each topic to provide the user guidance on each step of the enrollment process.

I. DNP OVERVIEW

The Do Not Pay Business Center provides services and support activities related to the identification, detection, and prevention of improper payments under the Improper Payments Elimination and Recovery Improvement Act of 2012 (IPERIA) and the Federal Improper Payments Coordination Act of 2015 (FIPCA).

- The Office of Management and Budget (OMB) designated the Department of the Treasury to host the working system to assist agencies in detecting and preventing improper payments.

- The Bureau of the Fiscal Service (Fiscal Service) operates the DNP Business Center.

The mission of DNP is to protect the integrity of the federal government’s payment processes by assisting agencies in mitigating and eliminating improper payments in a cost-effective manner while safeguarding the privacy of individuals.

DNP provides multiple data sources so that agencies can verify eligibility of a vendor, grantee, loan recipient, or beneficiary. Agencies can make payment eligibility decisions at any time during the payment lifecycle for example, during pre-award and pre-payment eligibility verification.

- DNP is a no cost resource for federal agencies and federally funded state administered programs
- DNP is not a list of entities or people that should not be paid
- DNP offers customized data analysis to help agencies detect fraud, waste, and abuse as well as strengthen internal controls
- DNP meets existing federal data security and privacy standards
- DNP is committed to providing:
  - quality data
  - more data sources
  - continuous system development
  - cutting edge data analytics
  - customized agency outreach
DNP Business Center Components:

Web-based Portal
The DNP Portal provides the capability of multiple data source searches simultaneously. You can search for a single person or entity; you can batch your searches; and you can set up regular monitoring in the Portal.

The DNP Portal has four ways to deliver match information to an agency. The delivery method is based upon approved data sources and where in the payment lifecycle the match is reviewed.

- Online Search
- Batch Matching
- Continuous Monitoring
- Payment Integration

Data Analytics
Data Analytics provides advanced payment analysis to federal agencies. In partnership with the agencies, a variety of data analysis and visualizations can be conducted to help combat improper payments.

- Analyzes payment data for indicators that a payment is being made in error or is vulnerable to abuse
- Develops risk scoring to help agencies prioritize and manage reviewing and investigating cross-matches
- Screens payees for eligibility such as identifying deceased beneficiaries

Agency Support
Agency Support is made up of onboarding specialists, outreach liaisons, and a help desk. Agency Support works with agencies to meet program needs, determine and target the best DNP processes and data sources, and provide training, Portal demonstrations, and share knowledge. Agency Support hosts community of events to share best practices for addressing improper payments, as well as assist with business processes by helping agencies map DNP into existing business processes.
PIV Onboarding Process Overview

This is a high-level flowchart of the DNP PIV, CAC, and LincPass onboarding process. These steps are detailed within this document.
II. COMPLETING FORMS

Senior Agency Outreach Liaison Sends User Enrollment Form

Your agency’s Point of Contact (PoC) will receive an email from your Senior Agency Outreach Liaison after the access group has been created. This email will contain a User Enrollment Form that must be reviewed and completed for each anticipated Portal user. If an anticipated Portal user has an existing PIV, CAC, or LincPass Card for another U.S. Treasury application (e.g., SPS, JFICS, etc.), this must be indicated on the User Enrollment Form.

Access Group Administrator (AGA) Completes and Signs the User Enrollment Form

Your Senior Agency Outreach Liaison will populate all the “Internal Use Only” fields within your User Enrollment Form before sending to your agency. The remaining fields will need to be completed and the form must be signed by your agency’s designated AGA. Your agency’s Authorizing Official (AO), Primary Local Security Administrator (PLSA), or Local Security Administrator (LSA) can act as an AGA; AGAs designate which access group a user is permitted to view. The DNP Program requires that each page of your User Enrollment Form be returned to your Senior Agency Outreach Liaison. If there are questions regarding specific fields within your form, your Senior Agency Outreach Liaison can assist you.

Example of the User Enrollment Form:
III. EMAILS

DNP Rules of Behavior Email

After your user enrollment form has been returned to your Senior Agency Outreach Liaison, you will receive an email from the DNP email box (DoNotPay@fiscal.treasury.org), asking you to review and accept our Rules of Behavior (RoB). Please ensure that you thoroughly review the requirements and accept the terms. Acceptance is as easy as filling in your name and replying to the original email sent from DNP.

Example of the RoB Email:

---

A request was recently submitted to grant you access to the Do Not Pay Portal. Do Not Pay is a program of the Department of Treasury’s Bureau of the Fiscal Service.

*What You Need to Know*

Users of the Do Not Pay Portal are required to accept the attached Rules of Behavior before access can be granted.

*What You Must Do*

Accept the mandatory Rules of Behavior requirement by following the instructions below.

- Review the attached Do Not Pay Rules of Behavior.
- Complete the confirmation statement below by inserting your full name into the statement thus confirming you agree to the Rules of Behavior.
- Reply with the completed confirmation statement to DoNotPay@fiscal.treasury.org by [insert date].

***Note: Once you receive access you must login within 30 days or your access will be automatically deleted.***

You must reply by [insert date] to avoid having your access to Do Not Pay denied.

Confirmation Statement:

1, [**insert full name here**], have read and agree to the attached document in accordance with the Do Not Pay Rules of Behavior requirement.

***Note: By replying to this email with a confirmation statement, you are stating that you agree to the Rules of Behavior for Do Not Pay.***
Example of the attached RoB Document:

IBM Security Identity Manager (ISIM) Email

After you have accepted DNP’s RoB, your User Enrollment Form will move to the user provisioning phase. Before granting access to the Portal, you must have an ISIM account. After your account has been provisioned, you will receive two automated emails; one with your ISIM User ID and one with a temporary ISIM password. You must login to create your ISIM password. **You have 24 hours to create an ISIM password; if not, the temporary password must be reset.**

In ISIM, you will be reminded on the Single Sign On page that by logging in, you agree to abide by the Rules of Behavior. A link will also be available that will direct you to review the Rules of Behavior. There is a set of Rules for both Internal and External Users.
You can either scroll or click the appropriate box to review the Rules of Behavior that apply to you.

You will receive the following two emails. The first email includes your ISIM User ID while the second includes your temporary ISIM password. For security purposes, they are sent separately.

**Example of ISIM Emails:**
How to Create Your ISIM Single Sign On ("SSO") Password

The following instructions will assist you in creating your ISIM SSO password.

1. By clicking the link on the second email, it will take you to the Single Sign On page where you will enter your User ID and temporary password received in the email and click [Login].

2. You will then be directed to change your password by entering the temporary password again and then your new password following the rules listed. After changing your password click [Change Password].

#### 2. Review the criteria for my new password:

- Maximum repeated characters: 2
- Reversed history length: 10
- Minimum alphanumeric characters: 2
- Repeated history length: 10
- Disallow user ID: True
- Disallow user name(with Case-Insensitivity): True
- Disallow user name: True
- Maximum length: 15
- Required characters: [@#$%^()_+=]
- Disallow user ID(with Case-Insensitivity): True
- Minimum numeric characters: 1
- Minimum length: 12
3. You will receive confirmation that this will be the password to use the next time you log in. Click [Continue] to complete the Challenge/Response steps.
4. Next you will need to complete the Challenge/Response information. The responses to these questions will help validate your identity for future password resets. Select the check box next to the three questions you want to answer and type your answer in the Response field as well as the Confirm Response field. After responding to three of the six questions, click [Save My Questions & Responses].

5. You will now need to enter your Shared Secret. The Shared Secret is used to assist the help desk validate your identity if you need your password reset but have forgotten your Challenge/Response information. Your Shared Secret is required to be at least 3 characters long and should be a word or phrase that is easy for you to remember. After populating and confirming your Shared Secret, click [Save my Shared Secret].
6. The system confirms that your Challenge/Response and Shared Secret have been saved. You will be required to wait 15 minutes before you are able to log into ISIM again or your application for the first time.

7. Click the [Logout].

8. View of the ISIM Self-Service screen once the ISIM password has been successfully created.
How to Reset Your ISIM Single Sign On ("SSO") Password

The following instructions will assist you in resetting your ISIM SSO password.

1. Access the ISIM Self-Service website.
   
   URL – https://isim.fiscal.treasury.gov/itim/self

2. Enter your User ID and Password, and then click [Log In].

3. The ISIM Self-Service website will display.

4. Click [Change Password].
5. On the Change Password page, you will first need to select the accounts for which you would like to change the password. Click (1) [Select my accounts that will be affected by this password change].

6. All the accounts associated with your profile will appear. You can change the password for all your accounts or just select accounts. To synchronize the password on all your accounts in ISIM, click the Select All check box. If you only want to change your password for particular accounts only select the check box to the left of the account type.

7. Check the box next to [Single Sign On (FSLDAP)] in the Account Type column.
8. Click ['Review the criteria for my new password'] to display the criteria for creating your new password. You must now enter your new password using the criteria outlined and then confirm the password by re-entering it. Click [OK] to change your password. If you do not want to change your password, click [Cancel] and you will be directed back to the Self-Service home page.

Note: If the Single Sign On account is not selected, the criteria for the password will not show when Option 2 is expanded.

9. Enter the new password in the New password field, confirm the password in the New password (confirm) field, and then click [OK].
10. The Request Submitted page shows the request detail of the action you just performed. To check the status of your request, click [View My Requests].

11. To verify your password was changed successfully click on the appropriate link in the Request Type column. The Status Detail shows the password change was successful. If you receive a Status Detail showing a failed request, you need to contact the Fiscal Service Help Desk at (304) 480-7777 for assistance to change your password.

12. Log off and log back in to test your new password.
Welcome to DNP Email

After the U.S. Treasury processes your form, you will receive the Welcome to DNP Email from the DNP email box (DoNotPay@fiscal.treasury.org). This email contains potential tools to ensure that you get the most out of the DNP Program and the Portal, and contact information for the DNP Support Center, if you should encounter issues attempting to log into the Portal (1-855-837-4391).

Example of the Welcome to DNP Email:

Dear New Do Not Pay User,

Welcome to Do Not Pay! Do Not Pay (DNP) is the no-cost robust analytics tool which helps federal agencies detect and prevent improper payments made to vendors, grantees, loan recipients, and beneficiaries. Agencies can check multiple data sources to make payment eligibility decisions.

We are excited to have you join us in the fight to detect and prevent improper payments. We want to know if you successfully logged in to the DNP Portal using your Personal Identity Verification (PIV) Card, Common Access Card (CAC), or LincPass Card.

Please contact the DNP Support Center (1-855-837-4391) immediately if you are having any login issues.

DNP Offers Several Educational Tools:
DNP Spotlight Training webinars, Computer Based Training (CBT) modules, and one-on-one training sessions are available and have been designed to ensure you get the most out of DNP. For example, the “How to Adjudicate in the Portal” CBT module and the “Introduction to DNP” (Spotlight Training) webinar are both tools that provide users step-by-step guidance and other relevant information.

Let Us Know How We Are Doing!
To ensure DNP is doing its best to assist you, please tell us about your experience throughout the enrollment process. Your feedback is incredibly valuable to the future delivery of customer service. You can contact us at donotpay@fiscal.treasury.org or 1-855-837-4391. In addition, our website has a lot of good information fiscal.treasury.gov/dnp.

We appreciate working with you and look forward to offering you our continued support.

Sincerely,

Do Not Pay Support Center
IV. GAINING ACCESS TO THE PORTAL USING A PIV CARD

PIV Card:
- Click [here](#) to move to the “Linking Your PIV Credentials” section within this Guide to link your PIV-I credentials before accessing the DNP Portal (*non-U.S. Treasury users*).
- If you are a U.S. Treasury employee using your PIV Card, click [here](#) to move to the “Logging into the DNP Portal” section within this Guide to assist you in logging into the DNP Portal.

Example of a PIV Card:

---

**Linking Your PIV Credentials**

Before Linking your PIV Credentials, Review Your “Certificate Authentication Status”

1. Insert your PIV Card.
2. Open a new internet browser window and navigate to [https://piv.treasury.gov](https://piv.treasury.gov).
3. Enter your PIV Card Pin and click [OK].
4. Your Certificate Authentication Status should read “SUCCESS”.

   If you do not see “SUCCESS”, this is indicative to a problem with your workstation or certificate. Please contact your local IT support for assistance.

1. Insert your PIV Card.
2. Open a new internet browser window and navigate to the CASS Home page.
   - URL - https://piv.treasury.gov/cass/
3. Click [I need to link my PIV or PIV-I cert to an existing Fiscal Service SSO account].
4. Enter first name, last name, and email address. These fields must match what the user already has in ISIM. Click [Submit].
5. You should receive an email with a registration link. Click the registration link.

![Registration Link Image]

6. Type in your ISIM User ID and Password.
   - If you have forgotten your password, contact the DNP Support Center at (855) 837-4391 to have your password reset.

![Password Entry Image]

7. You will receive an email from ISIM within a few minutes, confirming that your credentials were successfully linked. You can click on the link in the email or type in https://fiscal.treasury.gov/DNP/ and click [Log In].

![Success Confirmation Image]
V. LOGGING INTO THE DNP PORTAL

Open Your Internet Browser

1. Insert your PIV Card.
2. Type https://fiscal.treasury.gov/DNP/ in the address bar and push Enter.
3. Click [Log In].

Fiscal Service Enterprise Single Sign On

1) A new browser window will open.
   ➢ Click [PKI Log In].
2) Another browser window will open with your certificate information.
   - Select a Certificate and click [OK] and then enter your PIN associated with your PIV Card and click [OK].

3) Another browser window will open with DNP’s Terms and Conditions.
   - Please review the document and then click [Accept] to gain access to the application. This window will open each time you login.
DNP Portal: Homepage

In order to retain your access to the Portal you must follow the ISIM Aging Rules:

- **Suspended:** All user accounts that have not logged into the Portal in the last 120 days will have an account status change to “suspended”.
  - Suspended users must call the Treasury Support Center Help Desk at 1-855-837-4391 to have their account restored for access to the Portal.

- **Deleted:** All user accounts that have not logged into the Portal in the last 13 months will be “deleted”.
  - To regain access to the Portal, deleted users must complete the DNP enrollment process.

**Note:** If you no longer need access to the Portal, please contact your Authorizing Official, Primary Local Security Administrator, or your Local Security Administrator.

Redesigned Portal (Online Search is the only functionality that is currently available)
VI. USER GUIDE

For assistance navigating the DNP Portal, you may refer to the User Guide within the DNP Portal.

1. Log into the DNP Portal
2. Click on the (upper right corner)
3. A new window will open. Click [User Guide].
VII. TROUBLESHOOTING

Unable to Log into the DNP Portal

A. Verify the web address is correct. (https://fiscal.treasury.gov/DNP/)

B. Verify your version of Internet Explorer (Under Help > About Internet Explorer) – Internet Explorer (IE) 8, 9, and 11, Google Chrome, or Mozilla Firefox are supported.

C. Delete Temporary Internet Files (TIFs) and Cookies from Internet Explorer and restart Internet Explorer. (Tools > Internet Options > Browsing History – Delete > Delete Cookies, Delete Temporary Internet Files)

D. After re-opening Internet Explorer, please type https://fiscal.treasury.gov/DNP/ manually into your address bar.

E. If you are getting prompted for a PIV certificate, make sure you are choosing the correct certificate from the certificate box.

F. Verify you are inputting the Pin that you had set up for your PIV Card in the Password screen.

If you are still receiving an error, record the error message (a screenshot is best), and forward your name, ISIM User ID, phone number, email address, and a brief description of the problem in a secured email to the Do Not Pay email box or call the DNP Support Center at (855) 837-4391 for assistance.
Issues on Downloading Text or Excel File with Existing Browser

If the existing browser that is being used is preventing you from downloading a Text or Excel file, ensure that the browser settings under the Security section that reads “Do not save encrypted pages to disk” is checked. It depends on the browser version in use where this setting is located.

- Please see example below for Microsoft Internet Explorer (IE).
  - Specific for IE7, IE8, and IE9; it’s under Tools-> Internet Options -> Advanced Tab -> Security
### VIII. SYSTEM REQUIREMENTS

This section details the system and configuration requirements necessary to utilize the Portal.

<table>
<thead>
<tr>
<th>Requirement Type</th>
<th>Details</th>
</tr>
</thead>
</table>
| **System**       | - Web Browser: Internet Explorer 11 and Google Chrome  
                    **Note:** Please do not use the back button on your browser. DNP does not support the use of the browser back button. The navigation pane on the left side of the DNP Portal may be used to return to a previous screen.  
                    - Adobe Reader X and XI  
                    - Entrust Root Certificate: The Entrust (2048) Root Certificate must be installed in the “Trusted Root Certification Authorities” certificate store on the “local machine” (all user profiles) for the workstation. This certificate is normally installed by default with Internet Explorer. If it has been removed, you will need to have your agency reinstall the certificate.  
                    - Microsoft Excel versions 2003-2019  
                    **Note:** Excel downloads from DNP are in the Excel 2003 format but can be opened in later versions of Excel. Downloads are subject to Excel 2003 limit of 65,000 rows, so files larger than that may be truncated.  
                    - Internet Options Security Settings  
                    - Active Card Reader  
                    - Windows Resolution: 1280 x 1024 or higher |
| **Hardware**     | - PIV, CAC, or LincPass Card  
                    - Active Card Reader |
IX. FREQUENTLY ASKED QUESTIONS (FAQs)

Q. **Why is gaining access to the DNP Portal such a time intensive process?**
   A. The primary reason it takes time to gain access to the Portal is due to the security measures DNP takes to ensure that data sent and received in our system is secure. As we review your enrollment request, there are several time intensive steps that may delay the process, some of which include: observing The Privacy Act of 1974 with regard to an enrollment request or reconciling your agency’s specific technology practices against others in our system, a process that can sometimes lend itself to unpredictable interfacing problems. Ultimately, DNP makes every effort to ensure that privacy and security risks are mitigated, a process that takes time and may attribute to a lengthy enrollment process.

Q. **What does it mean that I’ve been selected to be a user in the DNP Portal?**
   A. Your position plays a vital role in the payment cycle at your agency. As part of your agency’s ongoing efforts to reduce improper payments, your agency is verifying their payments through the DNP Portal. Contact your Authorizing Official to obtain additional details. If you are unsure who you are Authorizing Official is at your agency, call DNP (855) 837-4391 and we can help point you to the correct person at your agency.

Q. **What are Rules of Behavior and why are they needed?**
   A. Rules of Behavior (RoB) are required and provide good information security and raise security awareness. RoB describes standard practices needed to ensure safe, secure, and reliable use of information and information systems.

Q. **What should I do if I did not accept the Rules of Behavior within 10 days?**
   A. Access will be denied if acceptance is not received within 10 days. Send an email to donotpay@fiscal.treasury.org requesting further instructions to accept the Rules of Behavior.

Q. **Why do I need a PIV Card?**
   A. Your PIV Card Token is used to verify and certify that you are allowed access to the DNP Portal. Your PIV Card is a secondary layer of authentication, to protect your information and your agency’s data within the DNP Portal.

Q. **My initial log in did not occur within 30 days of being granted access to DNP. What will happen to my access?**
   A. You have 24 hours to create an ISIM password; if not, the temporary password must be reset. To retain access to the DNP Portal, you must login in at least every 120 days or your access will be suspended. If you do not login to the DNP Portal in 13 months, your access to the DNP Portal will be deleted.
Q. How do I learn how to use the Portal?
A. Go to the DNP website at www.fiscal.treasury.gov/DNP/ to utilize resources. There, you can sign up specifically for Spotlight training. These webinars give instructions on various DNP Portal functions and services offered. As a user, you should receive an email invitation for the training at the beginning of each month. Also, your liaison is always available for one-on-one training to fit your specific needs.

Q. What if I have a question about my match results in the Portal?
A. Contact the DNP Support Center or send an email requesting contact at the DNP mailbox, donotpay@fiscal.treasury.gov. Do not send Personally Identifiable Information (PII) or screen shots with PII via email.

Q. What should I do with my PKI Token if I converted to PIV access?
A. Return your PKI token to:

   Bureau of the Fiscal Service
   257 Bosley Industrial Park Drive
   Parkersburg Warehouse & OP Center Dock 1
   Attn: ICAM
   Mail Stop T2-A
   Parkersburg WV 26101

X. GETTING HELP
There are several ways you can obtain help when using the DNP Portal.

   You may contact your Senior Agency Outreach Liaison or the DNP Support Center:
   ☑ (855) 837-4391
   ☐ donotpay@fiscal.treasury.org.