



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

March 2022

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

 Agency Specialist Sends User Enrollment Form 6

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

III. EMAILS..... 7

 IBM Security Identity Manager (ISIM) Email 7

IV. GAINING ACCESS TO THE PORTAL USING A PIV CARD..... 18

 Linking Your PIV Credentials..... 18

V. LOGGING INTO THE DNP PORTAL..... 21

 Open Your Internet Browser 21

 Fiscal Service Enterprise Single Sign On..... 21

 DNP Portal: Homepage..... 23

VI. USER GUIDE..... 24

VII. TROUBLESHOOTING 25

 Unable to Log into the DNP Portal 25

 Issues on Downloading Text or Excel File with Existing Browser 26

VIII. SYSTEM REQUIREMENTS 27

IX. FREQUENTLY ASKED QUESTIONS (FAQs) 28

X. GETTING HELP 29

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 Card (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 [Payment Information Integrity Act of 2019 \(PIIA\)](#) 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) DNP Business Center operates the Working System.
- The mission of DNP is to assist agencies to make informed decisions in the identification, mitigation, and elimination of improper payments.
- The DNP vision is to provide innovative customer and data driven solutions that reduce the improper payment footprint across federally funded and state administered programs.

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
- Payments
- Webservice/Application Program Interface (API)

Data Analytics

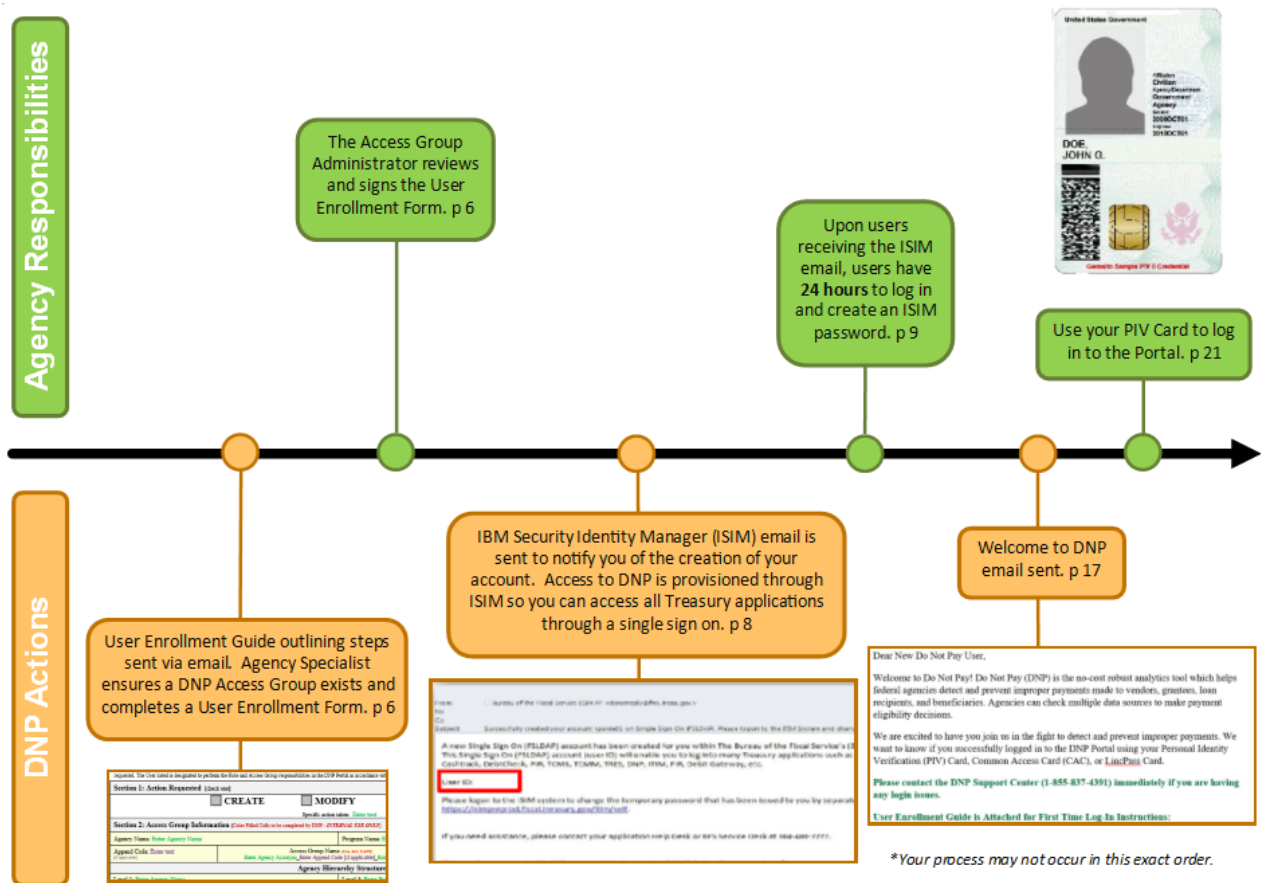
Data Analytics provides free advanced payment analysis service to federal agencies. In partnership with the agencies, a variety of data analysis and visualizations can be conducted to help combat improper payments.

- Analyze payment data for indicators that a payment is being made in error or is vulnerable to abuse
- Develop risk scoring to help agencies prioritize and manage reviewing and investigating crossmatches
- Screen payees for eligibility such as identifying deceased beneficiaries

Agency Support

Agency Support is made up of Agency Leads, Agency Specialists, onboarding specialists, and a help desk. Agency Support works with agencies to meet program needs, determine and target the best DNP processes and data sources. We provide training, Portal demonstrations, and share knowledge. Agency Support hosts community of events to share best practices for addressing improper payments. We also 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

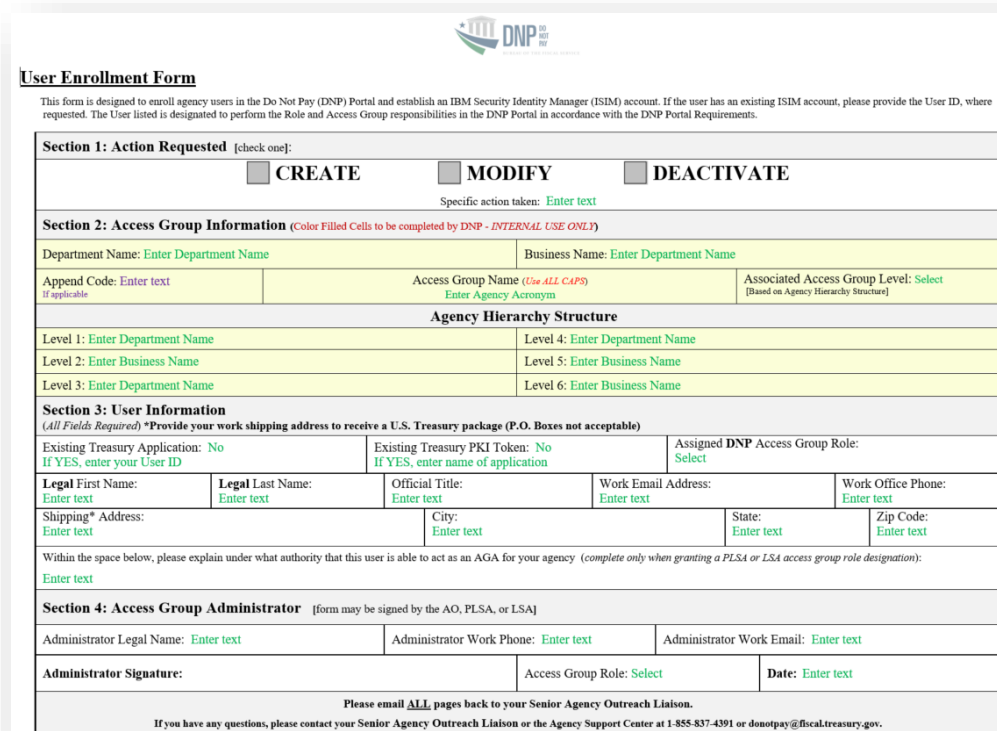
Agency Specialist Sends User Enrollment Form

Your agency's Point of Contact (PoC) will receive an email from your Agency Specialist 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 Agency Specialist 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 Agency Specialist. If there are questions regarding specific fields within your form, your Agency Specialist can assist you.

Example of the User Enrollment Form:



User Enrollment Form

This form is designed to enroll agency users in the Do Not Pay (DNP) Portal and establish an IBM Security Identity Manager (ISIM) account. If the user has an existing ISIM account, please provide the User ID, where requested. The User listed is designated to perform the Role and Access Group responsibilities in the DNP Portal in accordance with the DNP Portal Requirements.

Section 1: Action Requested [check one]:

☐ CREATE ☐ MODIFY ☐ DEACTIVATE

Specific action taken: Enter text

Section 2: Access Group Information (Color Filled Cells to be completed by DNP - INTERNAL USE ONLY)

Department Name: Enter Department Name Business Name: Enter Department Name

Append Code: Enter text Access Group Name (Use ALL CAPS) Associated Access Group Level: Select
if applicable Enter Agency Acronym (Based on Agency Hierarchy Structure)

Agency Hierarchy Structure

Level 1: Enter Department Name Level 4: Enter Department Name
Level 2: Enter Business Name Level 5: Enter Business Name
Level 3: Enter Department Name Level 6: Enter Business Name

Section 3: User Information
(All Fields Required) *Provide your work shipping address to receive a U.S. Treasury package (P.O. Boxes not acceptable)

Existing Treasury Application: No Existing Treasury PKI Token: No Assigned DNP Access Group Role: Select
If YES, enter your User ID If YES, enter name of application

Legal First Name: Enter text Legal Last Name: Enter text Official Title: Enter text Work Email Address: Enter text Work Office Phone: Enter text

Shipping* Address: Enter text City: Enter text State: Enter text Zip Code: Enter text

Within the space below, please explain under what authority that this user is able to act as an AGA for your agency (complete only when granting a PLSA or LSA access group role designation):
Enter text

Section 4: Access Group Administrator [form may be signed by the AO, PLSA, or LSA]

Administrator Legal Name: Enter text Administrator Work Phone: Enter text Administrator Work Email: Enter text

Administrator Signature: Access Group Role: Select Date: Enter text

Please email ALL pages back to your Senior Agency Outreach Liaison.
If you have any questions, please contact your Senior Agency Outreach Liaison or the Agency Support Center at 1-855-837-4391 or donotpay@fiscal.treasury.gov.

III. EMAILS

IBM Security Identity Manager (ISIM) Email

After your User Enrollment Form is received from the AGA, the user provisioning phase begins. Before being granted 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. Note the Warning included at the bottom of the page.

You have successfully logged out.
Please close your browser to complete the logout process

By logging in with PIV, SecurID, or User ID/Password, you acknowledge that you have read, understand, and agree to abide by the [Rules of Behavior](#)

PIV Card or iKey

Please make sure your card/iKey is plugged into the reader



LOGIN WITH YOUR PIV

SecurID

User ID

Passcode

LOGIN

User ID & Password

User ID (ITIM)

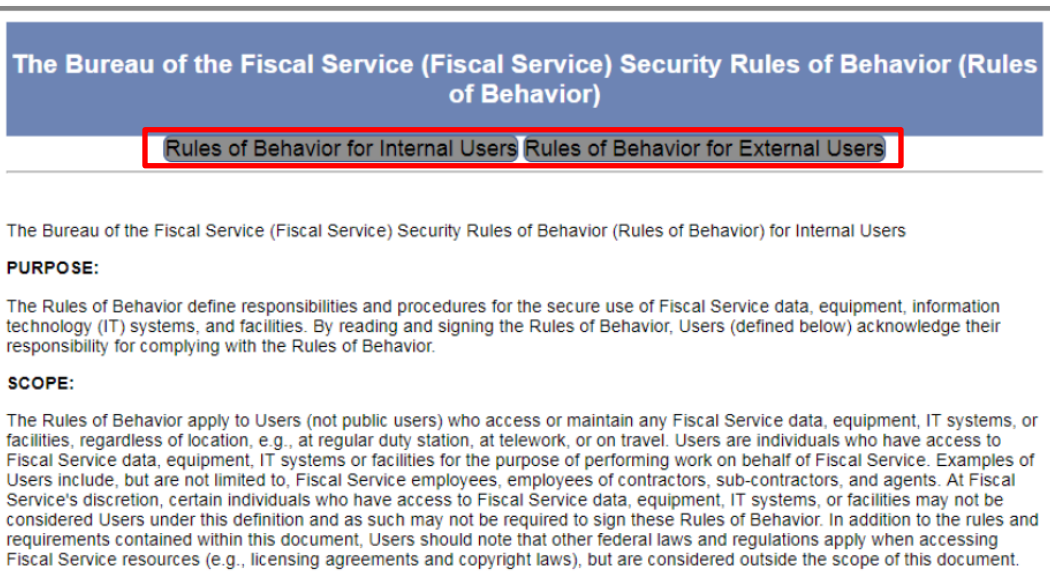
Password

LOGIN

WARNING WARNING WARNING

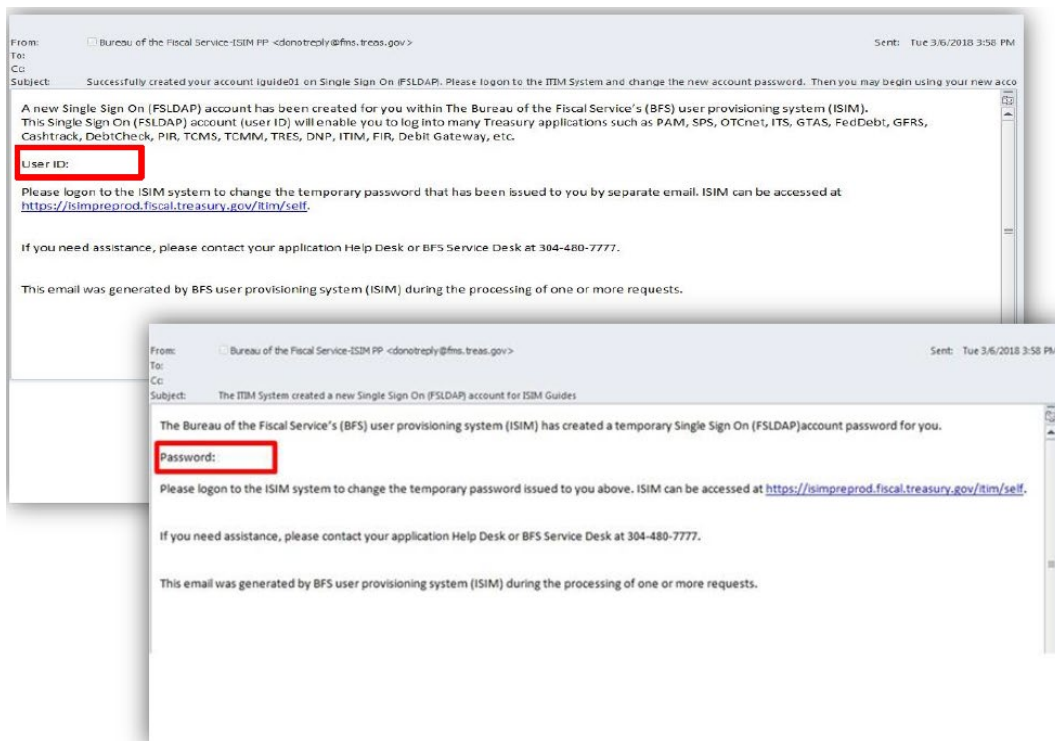
You have accessed a U.S. Government information system, which includes (1) this computer, (2) this network, (3) all computers connected to this network, and (4) all devices and storage media attached to this network or to a computer on this network. U.S. Government information systems are provided for the processing of official U.S. Government information only. Unauthorized or improper use of this information system is prohibited and may subject you to disciplinary action, as well as civil and criminal penalties. All data contained on U.S. Government information systems is owned by the U.S. Government and may, for the purpose of protecting the rights and property of the U.S. Government, be monitored, intercepted, recorded, read, searched, copied, or captured in any manner and disclosed or used for any lawful government purpose at any time. THERE IS NO RIGHT TO PRIVACY IN THIS SYSTEM. System personnel may give to law enforcement officials any potential evidence of crime found on U.S. Government information systems. USE OF THIS SYSTEM BY ANY USER, AUTHORIZED OR UNAUTHORIZED, CONSTITUTES YOUR UNDERSTANDING AND CONSENT TO THIS MONITORING, INTERCEPTION, RECORDING, READING, COPYING, OR CAPTURING AND DISCLOSURE.

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]**.

Single Sign On

Forgot Password Change Password Forgot User ID Contact

By logging in with PIV, SecurID, or User ID/Password, you acknowledge that you have read, understand, and agree to abide by the [Rules of Behavior](#)

PIV Card or iKey

Please make sure your card/iKey is plugged into the reader

LOGIN WITH YOUR PIV

SecurID

User ID

Passcode

LOGIN

User ID & Password

User ID (ITIM)

tisuser06

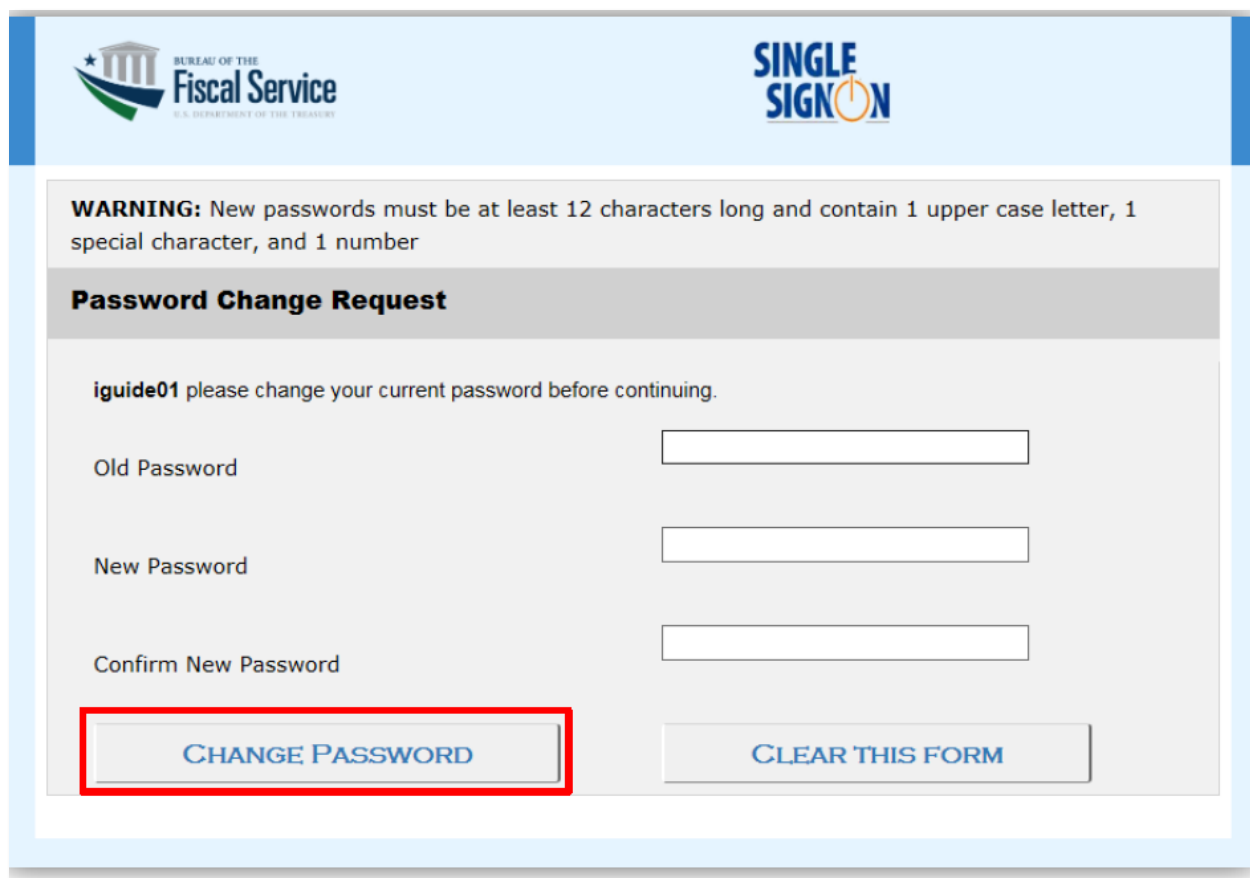
Password

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 alphabetic 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



The screenshot shows the 'Password Change Request' form. At the top left is the 'BUREAU OF THE Fiscal Service' logo, and at the top right is the 'SINGLE SIGN ON' logo. A warning message states: 'WARNING: New passwords must be at least 12 characters long and contain 1 upper case letter, 1 special character, and 1 number'. The form title is 'Password Change Request'. Below the title, a message says 'iguide01 please change your current password before continuing.' There are three input fields: 'Old Password', 'New Password', and 'Confirm New Password'. At the bottom, there are two buttons: 'CHANGE PASSWORD' (highlighted with a red box) and 'CLEAR THIS FORM'.

BUREAU OF THE Fiscal Service
U.S. DEPARTMENT OF THE TREASURY

SINGLE SIGN ON

WARNING: New passwords must be at least 12 characters long and contain 1 upper case letter, 1 special character, and 1 number

Password Change Request

iguide01 please change your current password before continuing.

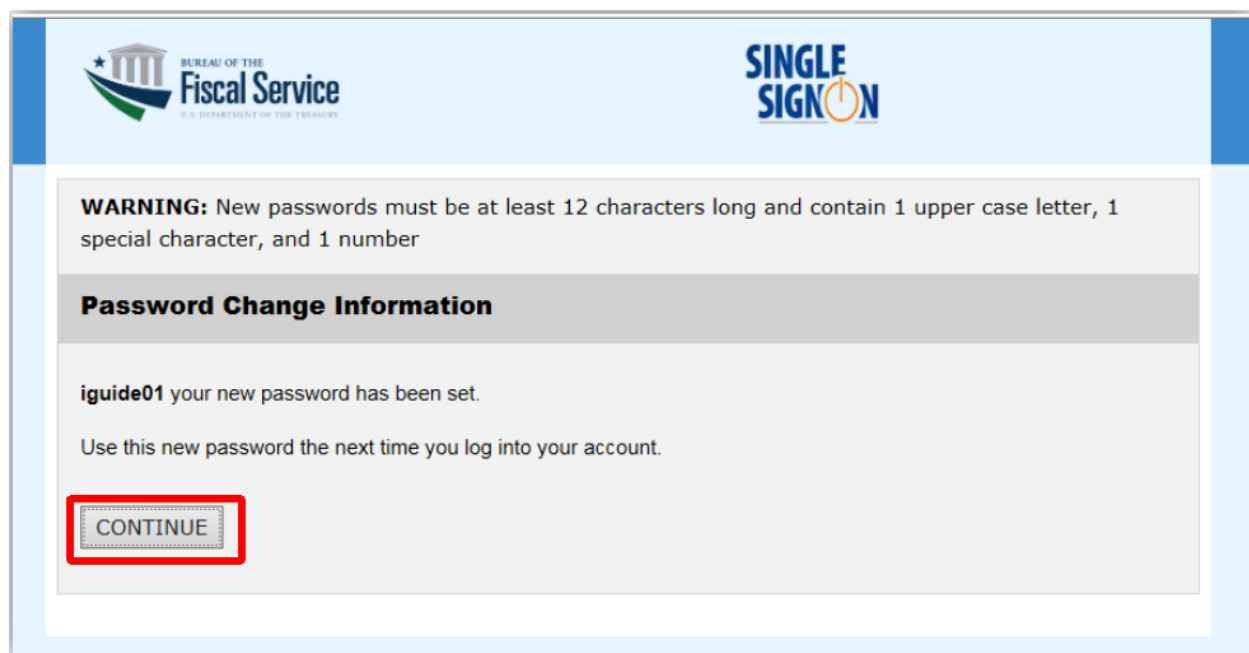
Old Password

New Password

Confirm New Password

CHANGE PASSWORD **CLEAR THIS FORM**

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.



The screenshot shows the 'Password Change Information' confirmation screen. At the top left is the 'BUREAU OF THE Fiscal Service' logo, and at the top right is the 'SINGLE SIGN ON' logo. A warning message states: 'WARNING: New passwords must be at least 12 characters long and contain 1 upper case letter, 1 special character, and 1 number'. The form title is 'Password Change Information'. Below the title, a message says 'iguide01 your new password has been set.' followed by 'Use this new password the next time you log into your account.' At the bottom, there is a button labeled 'CONTINUE' (highlighted with a red box).

BUREAU OF THE Fiscal Service
U.S. DEPARTMENT OF THE TREASURY

SINGLE SIGN ON

WARNING: New passwords must be at least 12 characters long and contain 1 upper case letter, 1 special character, and 1 number

Password Change Information

iguide01 your new password has been set.

Use this new password the next time you log into your account.

CONTINUE

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]**.

BUREAU OF THE Fiscal Service
U.S. DEPARTMENT OF THE TREASURY

Change Challenge/Response

Change Challenge/Response - Select and Provide Responses to Questions

If you forget your password or your password expires, you can choose to use our Self-Service Account/Password Reset process to reset it by clicking on the Forgot Password link on the login page. This process will ask you to provide the responses to the Challenge/Response questions you set up when you first accessed your account. This screen allows you to provide the responses that the Self-Service Account/Password Reset process requires. Select and provide responses to any 3 of the challenge questions below. Please ensure that each response is unique and at least 3 characters long and then click Save My Responses. Note: Responses are case-insensitive responses to any 3 of the challenges below, ensuring each response is unique and at least 3 characters long, and then click Submit. Note that responses are letter case-insensitive.

Select Question	Response	Confirm Response
<input type="checkbox"/> What was the name of the hospital where you were born?		
<input type="checkbox"/> What was the name of the street you lived on when you grew up?		
<input type="checkbox"/> What was the name of the company or organization where you held your first job?		
<input type="checkbox"/> What was the name of the city where you were born?		
<input type="checkbox"/> What was the name of your first pet?		
<input type="checkbox"/> What was the model of your first automobile?		

Save My Questions & Responses Cancel

[Accessibility](#) | [Contacts](#) | [Privacy Policy](#)
U. S. Department of the Treasury - Bureau of the Fiscal Service

5. You will now need to enter your Shared Secret. The Shared Secret is used to assist the Fiscal Service 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]**.

BUREAU OF THE Fiscal Service
U.S. DEPARTMENT OF THE TREASURY

Change Shared Secret

Change Shared Secret - Set a new Shared Secret (used when calling the Help Desk)

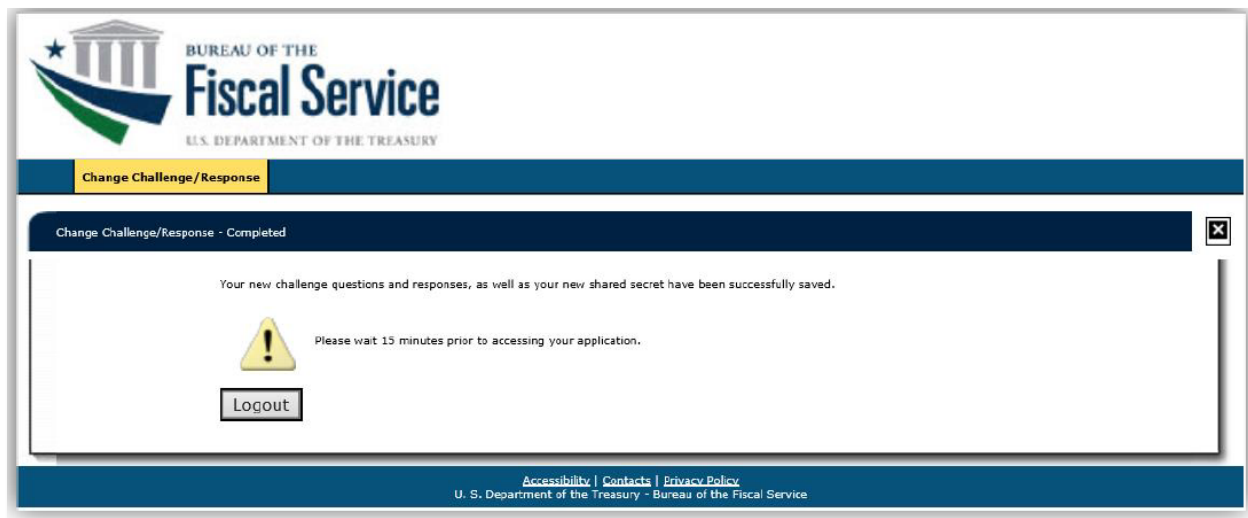
Your Shared Secret is used by the Help Desk personnel to verify your identity when you call them. At that time, you need to provide this shared secret. This screen allows you to set the Shared Secret phrase. Please ensure that the shared secret is at least 3 characters long and then click Save My Shared Secret button.

Shared Secret	Confirm Shared Secret

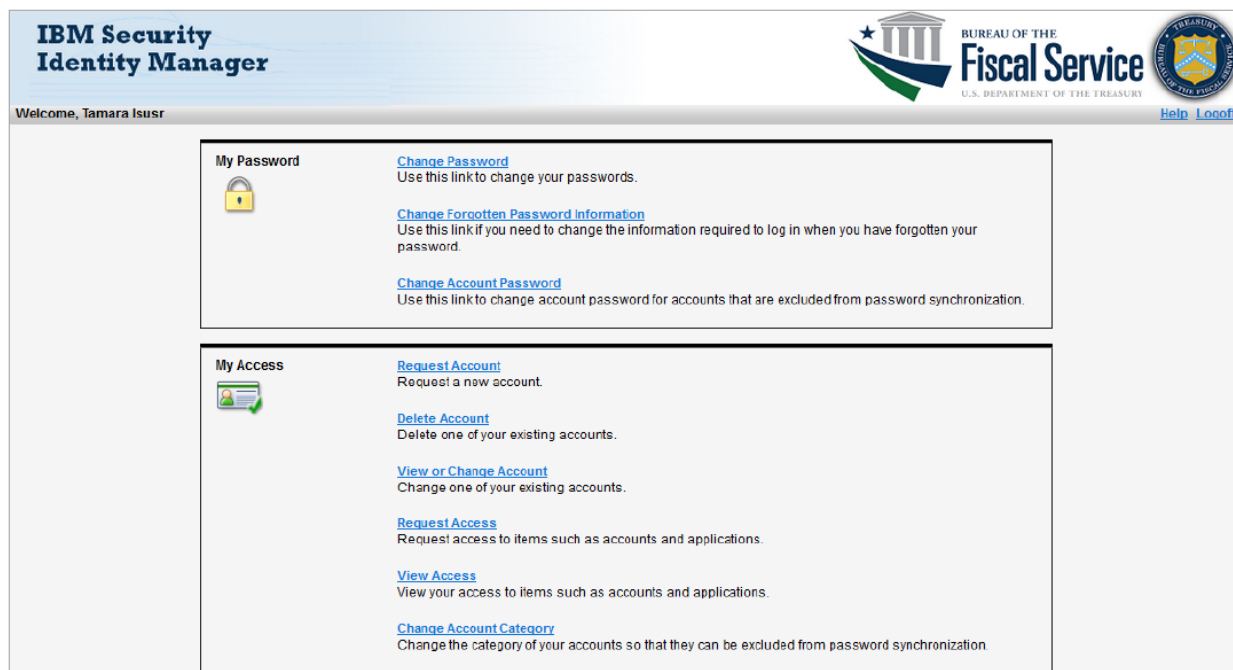
Save My Shared Secret Cancel

[Accessibility](#) | [Contacts](#) | [Privacy Policy](#)
U. S. Department of the Treasury - Bureau of the Fiscal Service

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]**.

- 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]**.

IBM Security Identity Manager

Welcome, Tamara Isusr
[Home](#) > [Change password](#)

Change Password

Select the accounts to be affected by the password change, then review the criteria for the new password, then specify a new password in the fields below and click OK to change your password. Click the Cancel button to cancel without changing your password.

▶ **1. Select my accounts that will be affected by this password change.**

▶ **2. Review the criteria for my new password:**

3. Change my password

New password:

New password (confirm):

- 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.
- Check the box next to **[Single Sign On (FSLDAP)]** in the Account Type column.

IBM Security Identity Manager

Welcome, Tamara Isusr
[Home](#) > [Change password](#)

Change Password

Select the accounts to be affected by the password change, then review the criteria for the new password, then specify a new password in the fields below and click OK to change your password. Click the Cancel button to cancel without changing your password.

▼ **1. Select my accounts that will be affected by this password change.**

<input type="checkbox"/> Select All	User ID	Account Type	Description
<input type="checkbox"/>	tsusr08	Single Sign On (TWAJ IT)	
<input type="checkbox"/>	tsusr08	Single Sign On (TWAJ FT)	FSLDAP at TWAJ FT
<input type="checkbox"/>	tsusr00	Single Sign On (FSLDAP)	This Single Sign On (FSLDAP) account (user ID) will ene...

Page 1 of 1 Total: 3 Displayed: 3 Selected: 0

Search for accounts
 Cannot find the account you are looking for? [Search](#) for more accounts.

▶ **2. Review the criteria for my new password:**

3. Change my password

New password:

New password (confirm):

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]**.

Change Password

Select the accounts to be affected by the password change, then review the criteria for the new password, then specify a new password in the fields below and click OK to change your password. Click the Cancel button to cancel without changing your password. All required fields are marked with (*).

▼ 1. Select my accounts that will be affected by this password change.

Select	User ID	Account Type	Description
<input checked="" type="checkbox"/>	tsur06	Single Sign On (TWAI FT)	
<input checked="" type="checkbox"/>	tsur06	Single Sign On (TWAI FT)	FSLDAP at TWAI FT
<input checked="" type="checkbox"/>	tsur06	Single Sign On (FSLDAP)	This Single Sign On (FSLDAP) account (user ID) will ens...

Page 1 of 1 Total: 3 Displayed: 3 Selected: 3

Search for accounts
Cannot find the account you are looking for? [Search](#) for more accounts.

⇒ 2. Review the criteria for my new password:

Maximum repeated characters	2
Reversed history length	10
Minimum alphabetic 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. Change my password

+New password:

+New password (confirm):

OK Cancel

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]**.

IBM Security Identity Manager

Welcome, Tamara Isusr

[Home](#) > [Change password](#) > Request submitted

Request Submitted: Change Password

You have submitted a request. Below is the information available to you at this time.

Request Detail

Request ID: 956501334221918061

Date Submitted: April 3, 2018 3:50:09 PM

Request Type: Change Password for Multiple Accounts

Access/Account: tisu06 on Single Sign On (TWAJ IT)
tisu06 on Single Sign On (TWAJ FT)
tisu06 on Single Sign On (FSLDAP)

Related Tasks

To check on the status of your request, refer to the [View My Requests page](#).

To perform other tasks go to the [IBM Security Identity Manager Home page](#).

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.

View My Requests

Click the request type to view its information.

View: Show last 31 days

Request Type	Date Submitted	Status	Account/Access
Change Password for Multiple Accounts	2018 04 03 15:50:09	Success	tisu06 on Single Sign On (FSLDAP), tisu06 on Sin...
Delete Account	2018 04 03 12:56:50	Success	tisu06 on TCIS QA
Account Change	2018 04 03 13:19:20	Timed Out	tisu06 on PPS
User Data Change	2018 04 03 11:31:47	Success	Tamara Isusr
Account Add	2018 04 03 11:10:50	In Process	null on null
Account Change	2018 03 22 09:26:59	Warning	tisu06 on GTAS
Account Add	2018 03 08 08:30:53	Failed	tisu06 on PPS (TWAJ QAC)
Account Add	2018 03 08 06:30:01		
Delete Account	2018 03 08 06:28:02		
Account Add	2018 03 08 06:27:59		

Page 1 of 1 Total: 10 Displayed: 10

[Go to Home Page](#)

Request Information

Request Detail

Request ID: 956501334221918061

Date submitted: April 3, 2018 3:50:09 PM

Request type: Change Password for Multiple Accounts

Account/Access: tisu06 on Single Sign On (FSLDAP)
tisu06 on Single Sign On (TWAJ FT)
tisu06 on Single Sign On (TWAJ IT)

Date completed: April 3, 2018 3:51:16 PM

Status Detail: Success

[Go to View My Requests](#)

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@stls.frb.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 (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 (855-837-4391) immediately if you are having any login issues.

DNP Offers Several Educational Tools:

DNP Video Trainings 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” and the “Introduction to DNP” on-demand videos are tools that provide users step-by-step guidance and other relevant information. To access these tools, go to <https://fiscal.treasury.gov/dnp/training.html>.

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.gov or 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.

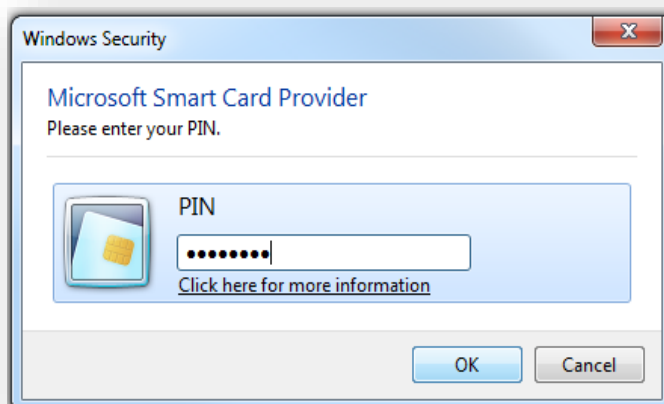
Example of a PIV Card:



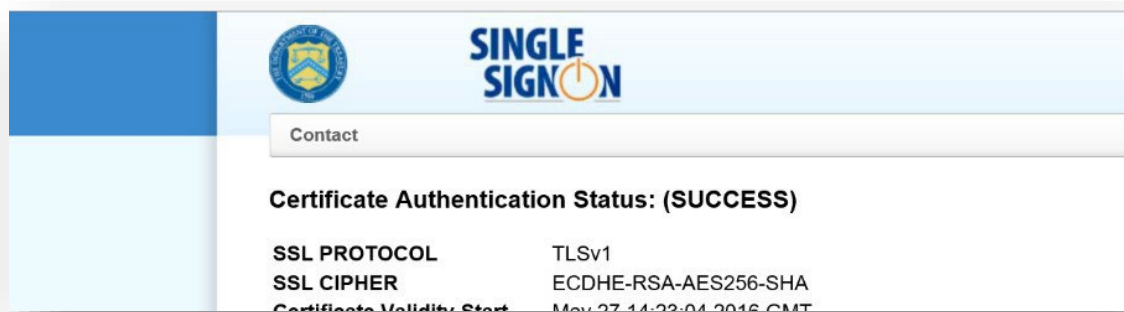
Linking Your PIV Credentials

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>.
3. Enter your PIV Card Pin and click [OK].



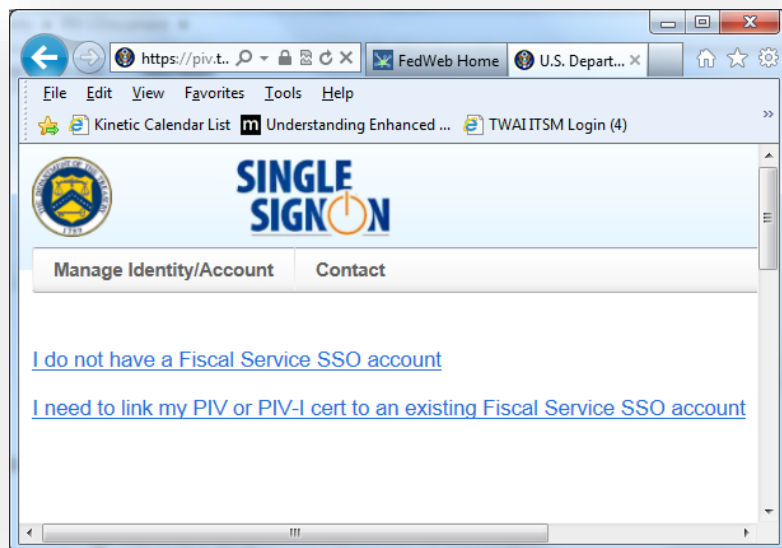
4. Your Certificate Authentication Status should read “SUCCESS”.



- 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.

Linking Your PIV Credentials:

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]**.

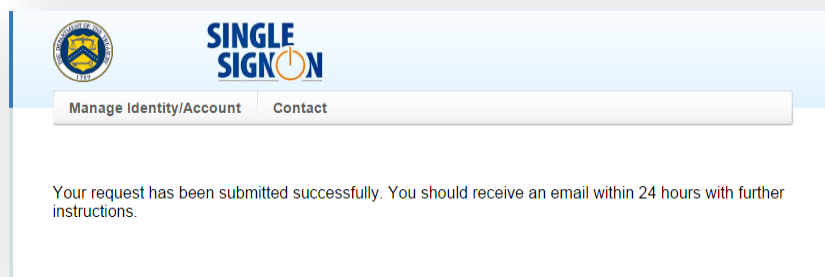
5. You should receive an email with a registration link. Click the registration link.



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.

A screenshot of the SINGLE SIGN ON web interface. At the top left is the Department of the Treasury seal. To its right is the 'SINGLE SIGN ON' logo. Below the logo are two tabs: 'Manage Identity/Account' and 'Contact'. The main content area contains the text: 'Enter the userID and password for the SSO account you wish to link to your PIV or PIV-I credentials'. Below this text are two input fields: 'UserID:' and 'Password:'. Below the input fields is a 'Submit' button.

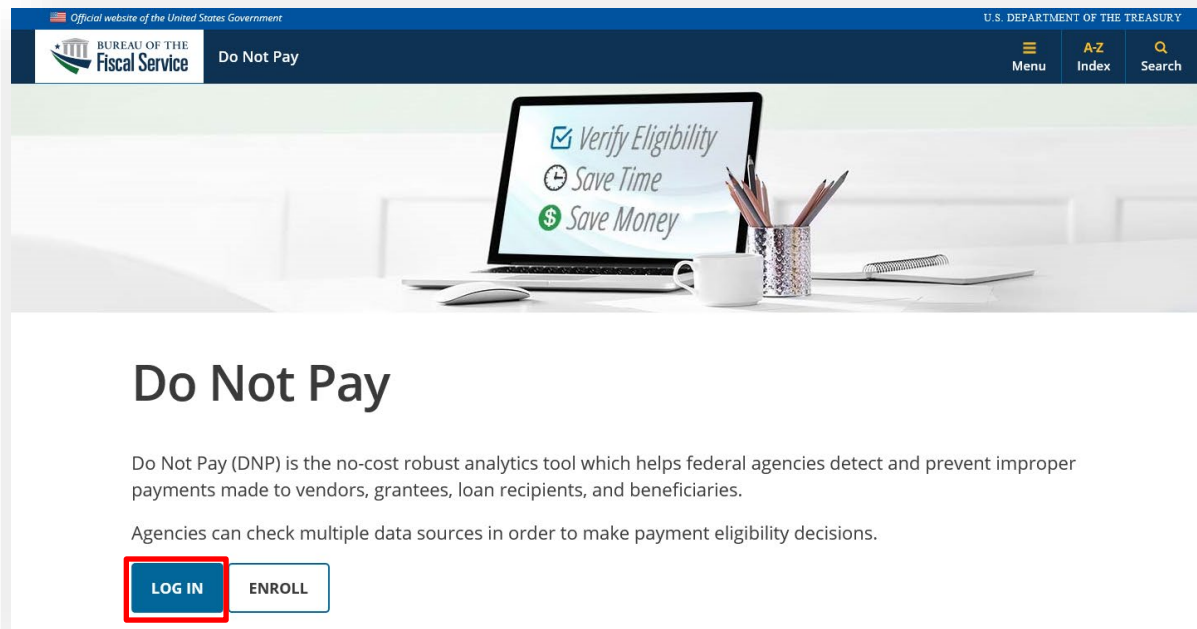
7. You will receive an email from ISIM within a few minutes, confirming that your credentials were successfully linked. You can click on the link in the email or type in <https://fiscal.treasury.gov/DNP/> and click **[Log In]**.



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]**.

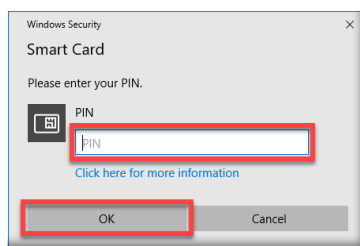
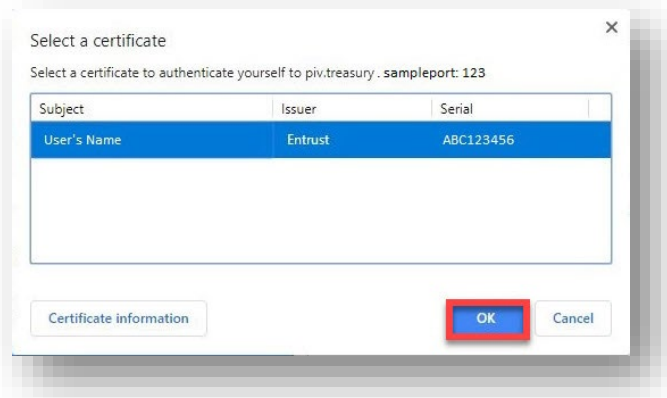


Fiscal Service Enterprise Single Sign On

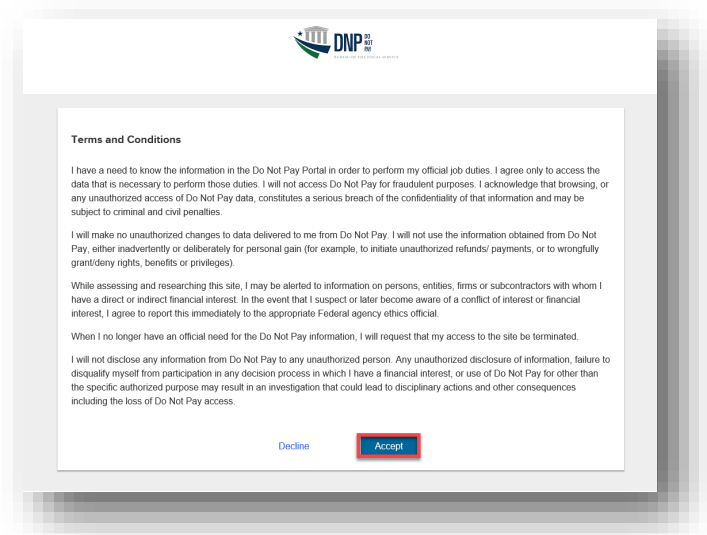
- 1) A new browser window will open.
 - Click **[Login with Your PIV]**. Note your agreement to the Rules of Behavior.



- 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]**. Your screen may look different based on your Windows version.



- 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:

- **ISIM Password Reset:** Each user must reset their Single Sign On password at least every 120 days, even if you are logging into the Portal using a PIV card or PKI token. To reset your password go to [ISIM Self Service](#).
 - Once the 120 days has lapsed, you cannot login to ISIM to reset your password; you must call the Help Desk at 855-837-4391 to have it reset.
- **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 DNP Support Center at 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.

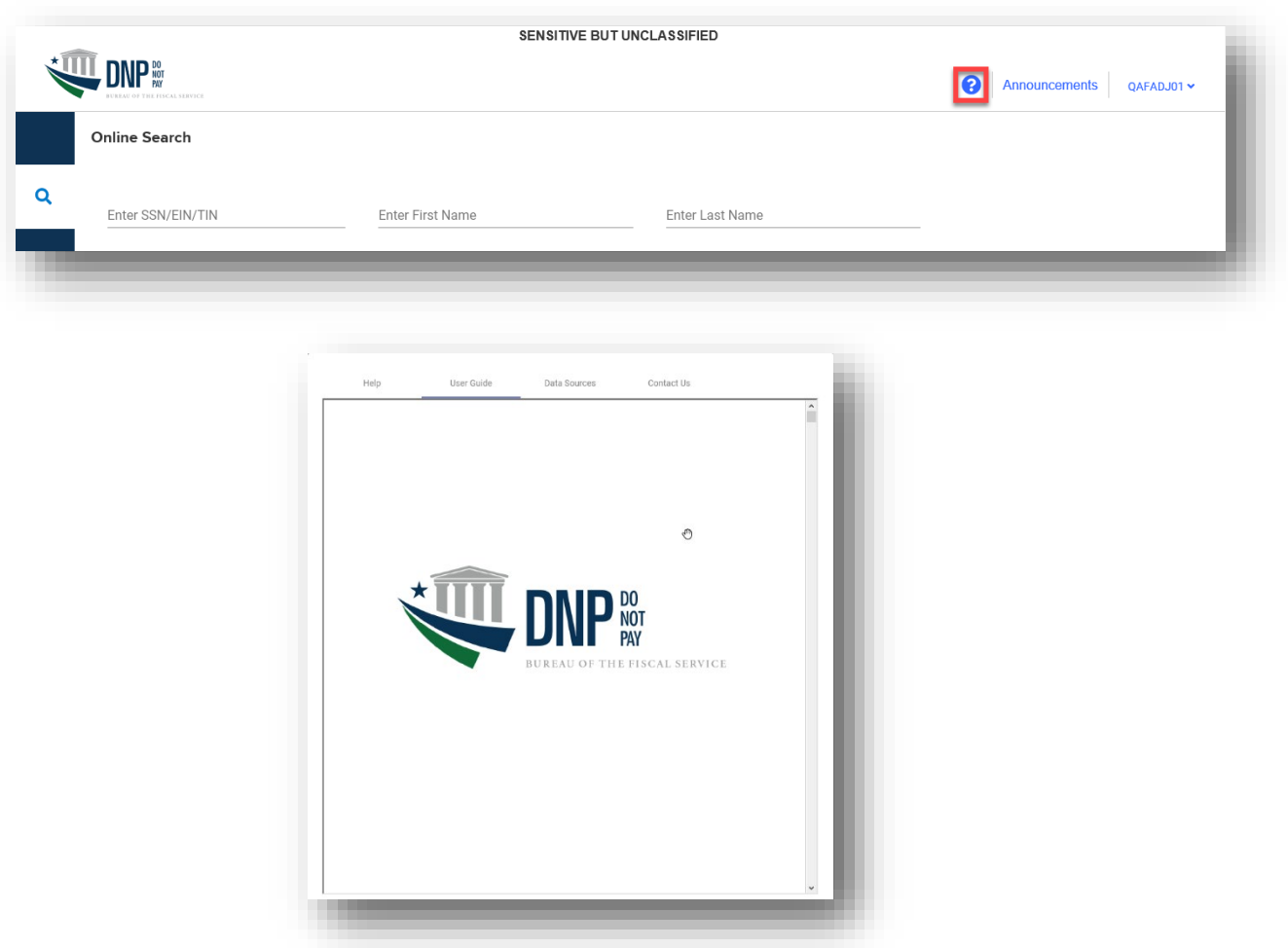
Redesigned Portal

The screenshot displays the DNP Portal homepage. At the top, it is labeled "SENSITIVE BUT UNCLASSIFIED". The header includes the DNP logo, a "DO NOT PAY" badge, and navigation links for "Announcements", "INT_CBAFWLONE", and "MCSR0001". A sidebar on the left contains icons for search, documents, infinity, a plus sign, a list, and a folder. The main content area features an "Online Search" section with input fields for "Enter SSN/EIN/TIN", "Enter First Name", "Enter Last Name", "Enter UEI", "Enter EFT Indicator", "Enter Business Name", "Enter DUNS", and "Enter Plus 4". A "Search" button and a "Clear" button are located to the right of these fields. Below the search fields is a "Select Data Sources" dialog box with a list of checkboxes for various data sources, all of which are currently checked. The dialog box is titled "Select Data Sources" and has a close button (X) in the top right corner. The footer of the page includes the text "SENSITIVE BUT UNCLASSIFIED" and "An Official Website of the United States Government".

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

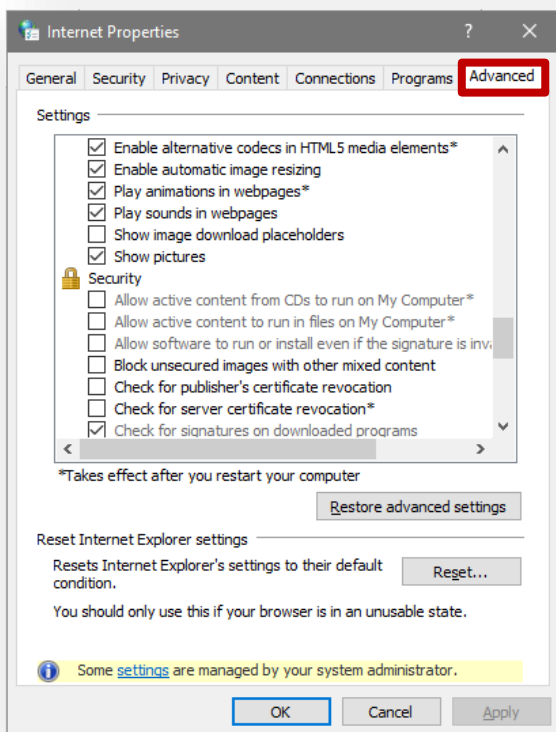
- A. Verify the URL is correct. (<https://fiscal.treasury.gov/DNP/>)
- B. Do not use Internet Explorer. You may use Microsoft Edge, Google Chrome, or Firefox.
- C. Delete Temporary Internet Files (TIFs) and Cookies from your browser.
- D. After re-opening your browser, please type <https://fiscal.treasury.gov/DNP/> 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 donotpay@stls.frb.org 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 Edge.
 - Go to Tools-> Internet Options -> Advanced Tab -> Security



VIII. SYSTEM REQUIREMENTS

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

Requirement Type	Details
System	<ul style="list-style-type: none"> Web Browser: Microsoft Edge, Google Chrome, or Firefox <p>Note: Microsoft Edge Native Mode which emulates Internet Explorer is not supported by DNP. 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 page.</p> <ul style="list-style-type: none"> Adobe Reader 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 2007 and later Internet Options Security Settings Windows Resolution: 1280 x 1024 or higher
Hardware	<ul style="list-style-type: none"> PIV, CAC, or LincPass card and 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 your Authorizing Official is at your agency, call the DNP Support Center at (855) 837-4391 and we can help point you to the correct person at your agency.

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. What do I need to do if my DNP access is inactive?

A. Call the DNP Support Center (855) 837-4391 and ask to have your DNP access reactivated. You must login to DNP immediately to retain an active status.

Q. How do I learn how to use the Portal?

A. Go to the [Training page](#) at the DNP website to utilize resources. There, you can review Spotlight training and how-to videos. These resources provide videos on various DNP Portal functions and services offered. Also, your Agency Specialist 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 Agency Lead, Agency Specialist, or the DNP Support Center:

☎ (855) 837-4391

✉ donotpay@fiscal.treasury.gov.