



# Registration/User Guide for VA Account Systems Access and PIV Card Procedures for Non-Federal Employees

Indianapolis VA Regional Office

May 26, 2017

This document contains the necessary information for obtaining VA Systems Access for Accredited/Non-Accredited, Co-Located and/or Remote Veteran Service Officers (VSO), County Veteran Service Officers (CVSO), Private Attorneys, and VSO Administrative Staff.

## TABLE OF CONTENTS

A. Introduction.....	3
Message from Director .....	3
Purpose.....	3
Points of Contact.....	3
B. Initial Access Request .....	4
Checklist.....	5
Specific Procedures.....	6
C. Maintaining VA Systems Access .....	10
D. Personal Identification Verification (PIV) Card Renewal.....	11
Checklist.....	11
Specific Procedures.....	11
E. Termination of Access and PIV Card .....	13
 <u>Attachments:</u>	
Attachment 1: Access Request Form.....	14
Attachment 2: Certification of TRIP Training.....	15
Attachment 3: Identity Documentation Criteria.....	16
Attachment 4: Do's and Don'ts for PIV Card Holders.....	19
Attachment 5: Logging into VPN/CAG (for remote users).....	20
Attachment 6: Loading Outlook and Configuring PIV Card.....	24
Attachment 7: Logging into SHARE and VBMS .....	26
Attachment 8: Useful Information and Training Links.....	27
Enclosure: (Required Forms).....	28
• Declaration for Federal Background Investigation for Affiliates and Volunteers	
• VA 0711	
• VBA 20-0344	

## A. Introduction

Message from the Director of the Indianapolis Regional Office:

In August of 2004, President George W. Bush issued Homeland Security Presidential Directive 12 (HSPD-12) which mandated new standards for secure and reliable personal identification for employees, contractors, and for those who require access to VA systems. The standards set forth in the Directive allow for verification of a person's identity and are strongly resistant to fraud, tampering, counterfeiting, and terrorist exploitation.

I do recognize that there are multiple steps in a complicated process that can seem arduous. That said, I ask all involved to remember that the PIV authentication process is a very important step in maintaining our national security and protecting our Veterans' personal information. Thank you for your cooperation.

### Purpose:

This guide has been created to assist you in obtaining, maintaining, and renewing VA Systems access and a Personal Identification Verification (PIV) badge through the Indianapolis VA Regional Office (VARO). The appropriate Checklists, along with specific instructions, will help to navigate the necessary requirements that are required to work through these processes.

### Points of Contact:

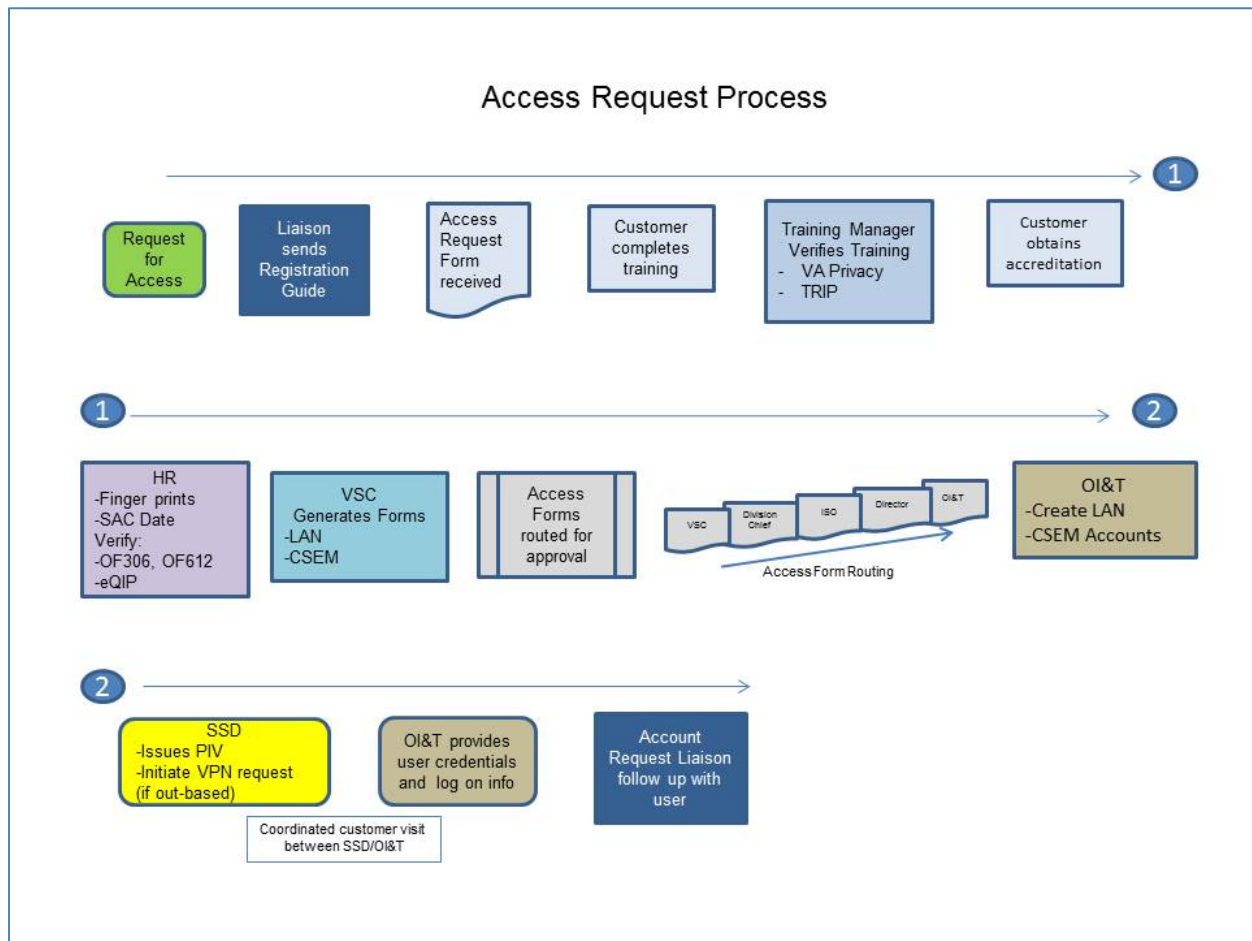
Table 1.

<b>POC</b>	<b>Assistance With...</b>	<b>Contact Info</b>
Account Request Liaison	General questions & status updates	(317) 916-3400
Indianapolis RO Training Manager	Training related issues	(317) 916-3400
Indianapolis Human Resources	Fingerprinting, security clearance, OF 306, OF 612, and eQIP questions	<a href="mailto:HR.VBAIND@VA.GOV">HR.VBAIND@VA.GOV</a>
Indianapolis Support Services	PIV badge issuance, and VPN/CAG request	<a href="mailto:SSD.VBAIND@va.gov">SSD.VBAIND@va.gov</a>
National Service Desk	Computer related issues	(855) 673-4357, option #3 then option #3 or email <a href="mailto:ITSC@va.gov">ITSC@va.gov</a>
National Citrix Access Gateway Help Desk	Logging into CAG for remote users	(855)673-4357, Option #6 then Option #1.

## B. Initial Access Request

This table shows an overview of the entire Access Request Process. Please allow 1-2 weeks to receive your PIV card and VA systems access after you complete the required training and forms.

Table 2.



The Initial Access Checklist beginning on page 5 will help you navigate through the process. Specific instructions for each step are provided on the pages following the checklist. If you have any questions, please contact the Account Liaison.

### INITIAL ACCESS CHECKLIST

- ☐ 1. Complete & fax Access Request Form (attachment 1) to **(215) 713-1112**.
- ☐ 2. Complete self-registration for a Talent Management System (TMS) account.
- ☐ 3. Complete TMS Training: VA Privacy and Information Security Awareness and Rules of Behavior. Notify the VARO Training Manager when complete.
- ☐ 4. Complete TRIP training (for accredited positions only). Upon completion, fax the Certification of TRIP Training Letter (Attachment 2) to **(215) 713-1112**.
- ☐ 5. Complete Accreditation. Notify the VARO Training Manager when complete.
- ☐ 6. Complete forms below and fax them to **(215) 713-1112**: (See enclosure, pg. 28)
  - Declaration for Federal Background Investigation for Affiliates and Volunteers
  - VA Form 20-0344, Annual Certification of Veteran Status & Veteran Relatives
  - VA Form 0711, Request for Personal Identification Verification Card
- ☐ 7. Complete fingerprinting for background investigation.
- ☐ 8. Complete all the required steps on the eQIP site within 10 calendar days from date email is received.
- ☐ 9. Schedule/receive Personal Identity Verification (PIV) card.
- ☐ 10. Receive VA Local Area Network (LAN) and email access.
- ☐ 11. (**Remote users only**) Obtain Virtual Private Network (VPN)/Citrix Access Gateway (CAG) account. This is used to log into the VA network from outside a VA facility. (See attachments 5 and 6 to log in)
- ☐ 12. Receive VA Applications access. Email will be automatically sent when you have access to VA Applications.
- ☐ 13. The Indianapolis Account Liaison will assist as needed.

**\*\*\*The number of each checklist item corresponds with numbered instructions below\*\*\***

## **INSTRUCTIONS**

1. Fill out and fax the Access Request Form (attachment 1) to **(215) 713-1112**. The information on this form is used to begin the process and help the VARO track your progress.
2. Self-register for the Talent Management System (TMS), the VA's online learning portal.

1.1. Go to <https://www.tms.va.gov>

1.2. Click on **Create New User**



1.3. Complete the VA TMS Self-Enrollment questions.

**Under MY JOB INFORMATION: (Enter the following information)**

- VA Location Code: **326(VBA Indianapolis Regional Office)**
- VA Point of Contact First Name: **Kyle**
- VA Point of Contact Last Name: **Schmidt**
- VA Point of Contact Email Address: [kyle.e.schmidt@va.gov](mailto:kyle.e.schmidt@va.gov)

1.4. Click Submit.

1.5. Go back to <https://www.tms.va.gov> and enter your User ID and Password. You are now logged into your TMS Home Page. (NOTE: you will need to log into TMS every year to complete the VA Privacy and Information Security course, so do not forget your User ID and password.)

3. You will be required to take VA Privacy and Information Security Awareness and Rules of Behavior training to establish and maintain your network access. The VA Privacy and Information Security Awareness and Rules of Behavior course will automatically be assigned when you create your TMS account. Upon completion of this training, please contact the VARO Training Manager, Kyle Schmidt, at [kyle.e.schmidt@va.gov](mailto:kyle.e.schmidt@va.gov).
4. **(Only accredited positions)** Federally mandated Training, Responsibility, Involvement and Preparation of Claims (TRIP) training will be coordinated by the

Indianapolis VARO Training Manager. Due to a contractual impairment, the TRIP training website located at [www.vsotrip.com](http://www.vsotrip.com) was taken offline on February 6, 2015. For the interim, Service Organizations are to have their Officers go through the material located at <https://www.sep.va.gov/web/guest/faq> and self-certify that they've completed the training. Once training is completed, fax the Certification of TRIP Training (Attachment 2) to **(215) 713-1112**. You will receive a TRIP certificate that you will need for accreditation.

5. You must be accredited by a recognized Service Organization (not required for non-accredited administrative positions). When you complete this process and receive confirmation from OGC, notify the Indianapolis RO Training Manager, [kyle.e.schmidt@va.gov](mailto:kyle.e.schmidt@va.gov)
6. Complete the following forms and fax them to **1-215-713-1112**. (See Required Forms starting on page 28) If you have any questions contact the Indianapolis Human Resources Office at (317) 916-3416.
  - [OF 306, Declaration for Federal Employment](#)
  - Current employment resume
  - VA Form 20-0344, Annual Certification of Veteran Status and Veteran Relatives
  - VA Form 0711, Request for Personal Identification Verification Card
7. Log onto the appointment scheduler website to make an appointment to take your fingerprints. [http://www.va.gov/PIVPROJECT/PIV\\_Badge\\_Offices.asp](http://www.va.gov/PIVPROJECT/PIV_Badge_Offices.asp)

**VERY IMPORTANT:** If you schedule an appointment anywhere *other than the Indianapolis Regional Office* please send an email to [SSD.VBAIND@va.gov](mailto:SSD.VBAIND@va.gov) and notify our office of the date and time of your appointment.

If you are getting fingerprinted at any other location *other than the Indianapolis Regional Office* you will need to provide the fingerprint office the following information:

-SON: 1074  
-SOI: VA11

8. When results of your fingerprint check are available, and you have submitted the OF306 and your Current Employment Resume, you will receive an e-mail message from HR with a link to the eQIP site. You must enter your information into the eQIP site and submit the information within 10 calendar days from the date of the e-mail. **IF YOU DO NOT COMPLETE** all of the necessary steps on the eQIP site within 10 calendar days from the e-mail, your account will need to be reactivated which could delay your receipt of a PIV card.

**NOTE: We will try to coordinate Steps 8-12 below to accommodate only one trip to the Regional Office. Please help us by making sure all steps are completed during your visit.**

9. Log onto the appointment scheduler website again to make an appointment to receive your PIV card. [http://www.va.gov/PIVPROJECT/PIV\\_Badge\\_Offices.asp](http://www.va.gov/PIVPROJECT/PIV_Badge_Offices.asp)

**VERY IMPORTANT:** If you schedule an appointment anywhere *other than the Indianapolis Regional Office* please send an email to [SSD.VBAIND@va.gov](mailto:SSD.VBAIND@va.gov) and notify our office of the date and time of your appointment. **If our office is not aware of your appointment at another facility then your PIV card may not get issued.**

Issuance of a PIV card is a three step process: 1) Sponsor 2) Registrar 3) Issuance.

- Sponsor: You will be contacted via telephone by the PIV Sponsor who will ask you a series of questions. This will take approximately 10 to 15 minutes.
  - Registrar: The PIV Registrar will ask for two forms of identification. The Registrar will enter this information into the PIV system and take your picture for the PIV card. Please see Attachment 3, Identity Document Criteria, before showing up to the PIV-issuing facility.
  - Issuance: The Issuer will ask you to provide one valid photo ID before printing and issuing your PIV card. You should inspect the card to verify your name is spelled correctly.
    - You need to provide a six-digit PIN number. This is the number you will enter in the computer when you log into VA information systems. It is recommended this be a series of numbers you can easily remember. If you forget your PIN number, you are required to visit a PIV-issuing facility to have it reset. This number **cannot** be reset remotely. It is encoded in the card's microchip and can only be reset by a PIV Issuer at his/her location.
    - Your PIV card contains certificates that allow you to read and send encrypted e-mails to anyone with a @va.gov e-mail address. You will receive instructions on safe handling of your card, how to use it with the VA e-mail system, and how to publish certificates to the VA Global Address List (GAL). When this has been accomplished, you are ready to use your new card.
10. The Indianapolis Office of Information and Technology (OI&T) will provide your credentials to log into the VA Local Area Network (LAN) if you are not PIV enforced. Beginning in January 2016 the VA is implementing 2 Factor Authentication



Enforcement (2FA) whereas most users will become PIV enforced. Your PIV card will be your primary means to log into the system. NOTE: You will need a PIV card reader to log into the system. A recommended reader is the Identiv SCR3310 V2 USB Smart Card Reader.

11. **(For remote users only).** You will be required to use VPN/CAG to log into the VA system from outside a VA facility. During steps 8 & 9 above, the Support Services Division, OI&T, and ISO will be requesting/approving your VPN account. Once you have your PIV card and VPN/CAG access you can follow the instructions in Attachments 5 and 6 to log into VPN/CAG, configure your PIV card and open Outlook.
12. Once your request for VA Applications has been approved you will receive an automatically generated email with your log on credentials. If you do not receive this email within one week of obtaining LAN access, please contact the Account Request Liaison.
13. The Indianapolis Account Request Liaison will make sure you have received positive support from all offices involved in the account access process. For more information or training links on the VBA systems, please see attachment 8.

### C. Maintaining VA Systems Access

Once you have received your PIV card, LAN access, email, and access to VA Applications you must stay active in the system. If any of the following items do not stay current, you may lose access and would need to reapply using the Initial Access Checklist.

- Remain current with required VA Privacy and Information Security Rules of Behavior training in TMS. This is an annual requirement.
- It is recommended to Log into CAG every 30 days to prevent being locked out.
- It is recommended to Log into VA Applications every 30 days to prevent being locked out.
- Maintain positive control of your PIV card. The card is solely for your use and must not be shared with anyone else.

If you are identified as not being active in one of the systems, the Indianapolis Veteran Service Center will contact you, either directly or through your servicing organization, regarding your status. If you no longer need access, or do not reply, the VARO will remove all VA systems access and disable your PIV card.

#### D. Personal Identification Verification Card Renewal

The process for PIV card renewal is similar to the initial card issuance process. The PIV Card Renewal Checklist and instructions will assist you through these steps.

##### PIV CARD RENEWAL CHECKLIST

- ☐ 1. Complete & fax the Access Request Form (attachment 1) to **(215) 713-1112**.
- ☐ 2. You must be current with TMS training, VA Privacy and Information Security Awareness Rules of Behavior.
- ☐ 3. Schedule/complete fingerprinting for background check.
- ☐ 4. The Indianapolis VARO will verify LAN and VA Applications accounts are current. If not current, LAN and CSEM will need to be resubmitted and routed for approval.
- ☐ 5. Schedule/receive new Personal Identity Verification (PIV) card.
- ☐ 6. **(Remote users only)**. Obtain Virtual Private Network (VPN)/Citrix Access Gateway (CAG) account. This is used to log into the VA network from outside a VA facility.

\*\*\*The number of each checklist item corresponds with numbered instructions below.\*\*\*

1. Fill out and fax the Access Request Form (attachment 1) to **(215) 713-1112**. This information is used to begin the process and help the VARO track your progress.
2. Log into TMS at <https://www.tms.va.gov> . Complete the VA Privacy and Information Security Awareness Rules of Behavior Training. All VA systems account access and PIV card will be deactivated if this training is not complete.
3. Log onto the appointment scheduler website to make an appointment to take your fingerprints. [http://www.va.gov/PIVPROJECT/PIV\\_Badge\\_Offices.asp](http://www.va.gov/PIVPROJECT/PIV_Badge_Offices.asp)

**VERY IMPORTANT:** If you schedule an appointment anywhere *other than the Indianapolis Regional Office* please send an email to [SSD.VBAIND@va.gov](mailto:SSD.VBAIND@va.gov) and notify our office of the date and time of your appointment.

If you are getting fingerprinted at any location *other than the Indianapolis Regional Office* you will need to provide the fingerprint office the following:

- SON: 1074      - SOL: VA11

4. Once the Indianapolis VARO receives confirmation of the SAC date from your fingerprints, the Indianapolis VARO will verify your LAN account and VA Applications are active. If not, the VARO will begin the approval process for activating your LAN and Applications accounts.
5. Log onto the appointment scheduler website again to make an appointment to receive your PIV card. [http://www.va.gov/PIVPROJECT/PIV\\_Badge\\_Offices.asp](http://www.va.gov/PIVPROJECT/PIV_Badge_Offices.asp)

**VERY IMPORTANT:** If you schedule an appointment anywhere *other than the Indianapolis Regional Office* please send an email to [SSD.VBAIND@va.gov](mailto:SSD.VBAIND@va.gov) and notify our office of the date and time of your appointment. **If our office is not aware of your appointment at another facility then your PIV card may not get issued.**

6. **(For remote users only).** You will be required to use VPN/CAG to log into the VA system from outside a VA facility. The Support Services Division, OI&T, and ISO will be requesting/approving your VPN/CAG account. You will receive a confirmation email notifying you that your VPN/CAG account is active. Instructions for logging into CAG and configuring your PIV badge can be found in attachments 5 and 6.

#### E. Termination of Access and PIV Card

If you resign, retire, or end affiliation with VA you are required to return your PIV card. Your PIV card is the property of the U.S. Government. Counterfeiting, altering, or misusing violates [Section 499, Title 18 of the U.S. Code](#). If you resign, retire, or end your affiliation with VA, you may not maintain possession of this federal property.

The PIV card should be returned to the Indianapolis VA Regional Office via certified mail.

The correct address is:

**Indianapolis VA Regional Office  
Attention: PCI Manager  
575 N. Pennsylvania St  
Indianapolis, IN 46204**

Attachment 1  
ACCESS REQUEST FORM



Indianapolis VA Regional Office Systems Access Request Form  
for  
VSOs, CVSOs, Private Attorneys, and Support Personnel

Please complete all the information below. This information will be used to create the VA Systems Access Forms and help the Regional Office track your progress through the process.

Please fax form to **(215) 713-1112**.

<b>Initial Access or Renewal?</b>	
<b>Name Last, First, MI.</b>	
<b>SSN</b>	
<b>Date of Birth (mm/dd/yyyy)</b>	
<b>Start Date (CVSO only) (mm/dd/yyyy)</b>	
<b>Telephone Number</b>	
<b>Email Address</b>	
<b>Service Organization or Firm</b>	
<b>Title</b>	
<b>Accreditation Number (If accredited)</b>	

If you have any questions, please contact the Account Access Liaison at (317) 916-3400.

Attachment 2  
CERTIFICATION OF TRIP TRAINING



**CERTIFICATION OF TRIP TRAINING**

I \_\_\_\_\_ from \_\_\_\_\_ certify that I have  
(Print Name) (Print Service Organization)

completed T.R.I.P. (Training, Responsibility, Involvement and Preparation of

Claims) Chapters 1-18 found at <https://www.sep.va.gov/web/guest/fag>

\_\_\_\_\_  
Employee Signature

\_\_\_\_\_  
Date

### Attachment 3

#### IDENTITY DOCUMENTATION CRITERIA

The following criteria must be met by all VA employees, contractors, and affiliates prior to being issued a PIV card or Non-PIV Card.

- The Registrar must examine each identity source document.
- All identity source documents must not be expired.
- The Registrar will reject any document that appears invalid (e.g., absence of security hologram, or other known security features, on a State issued driver's license; absence of security features on a birth certificate or passport; smeared ink; missing information; etc.), and this information will be reported to the Office of Security and Law Enforcement (OSLE) for review.
- Handwritten or photocopied documents are not acceptable.
- Two forms of identification are required from *Table 1: Acceptable Identity Documents*. The following combinations are accepted:
  - Two forms of identification from Column A (Government Issued Photo ID);
  - One form of identification from Column A and one form from Column B (Non-Picture ID or Acceptable Picture ID not issued by Federal or State Government)

Table 3. Acceptable Identity Documents

COLUMN A Government Issued Photo ID	COLUMN B Non-Picture ID and or Acceptable Picture ID not issued by Federal or State Government
<ul style="list-style-type: none"><li>• U.S. Passport or U.S. Passport Card</li><li>• Permanent Resident Card or Alien Registration Receipt Card (Form I-551)</li><li>• Foreign passport that contains a temporary I-551 stamp</li><li>• Employment Authorization Document that contains a photograph (Form I-766)</li></ul>	<ul style="list-style-type: none"><li>• Social Security Card</li><li>• Original or certified Birth Certificate</li><li>• Certification of Birth Abroad Issued by the Department of State (Form FS-545)</li><li>• Certification of Report of Birth issued by the Department of State (Form DS-1350)</li><li>• Voter's Registration Card</li><li>• Native American Tribal</li></ul>



<ul style="list-style-type: none"> <li>• Foreign passport with Form I-94 or Form I-94A</li> <li>• Passport from the Federated States of Micronesia (FSM) or the Republic of the Marshall Islands (RMI) with Form I-94 or Form I-94A</li> <li>• Driver's license or State issued ID card</li> <li>• Federal, state, or local government issued ID card</li> <li>• School ID with photograph</li> <li>• U.S. Military card</li> <li>• Military dependent's ID card</li> <li>• U.S. Coast Guard Merchant Mariner Card</li> </ul>	<p>Document</p> <ul style="list-style-type: none"> <li>• U.S. Citizen ID Card (Form I-197)</li> <li>• Identification Card for Use of Resident Citizen in the United States (Form I-179)</li> <li>• Employment Authorization document issued by the Department of Homeland Security</li> <li>• Canadian Driver's License</li> </ul>
---	--

### Applicant Names

The Applicant's name in the card request must be an exact match to the name printed on at least one of the identity source documents.

The names on the identity source documents must match using the examples in *Table 2: Acceptable Name Mismatches* and *Table 3: Unacceptable Name Mismatches*.

Applicants with multiple last names may use the guidance for middle names in *Table 2: Acceptable Name Mismatches*.

An ID issued before a legal name change (e.g. birth certificate or driver's license) can be presented as one form of ID if a legal document (e.g. marriage certificate/license or a court order) is also presented linking the previous name to the current legal name. The linking document has to display both the former and current legal names. Both documents must be valid (not expired).

For example, a married woman may use both a certified copy of her birth certificate that lists her maiden name and a driver's license showing her married name as long as she provides a marriage license displaying both her maiden name and married name.

Table 4. Acceptable Name Mismatches

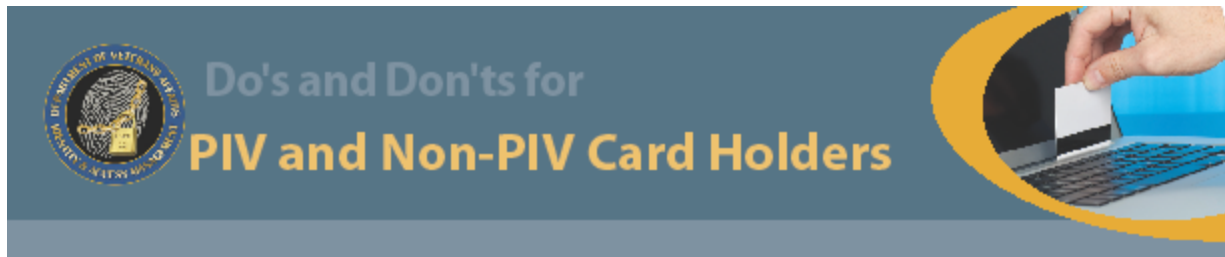
Name	Acceptable Mismatches	
	First Name Source Shows	Second Name Source Shows
First	Single first name  Example: "Mary" (with "L." given as middle initial)	First name as two words Example: "Mary Lou"
Middle	Single letter as middle initial  Example: "L."	Middle name spelled out, first letter of the name matches the single letter  Example: "Lawrence"
Last	Last name given in hyphenated form  Example: "Smith-Jones"	Last name given in non-hyphenated form  Example: "Smith Jones"

Table 5. Unacceptable Name Mismatches

Unacceptable Mismatches	First Name Source Shows	Second Name Source Shows
Apparent typo or transposition of letters in the name	"John"  "Smyth"	John"  "Smith"
Mismatch between given name and an alias or nickname	"Jim"	"James"
First and middle names swapped	"Eldon S. Smith"	"Scott Smith"
Mismatch of suffix	"Tom Smith Jr."	"Tom Smith"

## Attachment 4

### DO'S AND DON'TS FOR PIV CARD HOLDERS



Congratulations on getting your VA PIV/Non-PIV card! By caring for and using your card with integrity, you have the satisfaction of knowing that you are protecting the security, identity and privacy of not only yourself but of every single person at VA, VA as a whole, and the Veterans we serve.

Please follow these important guidelines for the proper care and use of your card.

## DO

- ✓ Keep your PIV or Non-PIV card in the VA-issued electromagnetically opaque card holder when you're not using it
- ✓ Remember your personally selected 6 digit PIN
- ✓ Use your PIV or Non-PIV card for physical access to buildings/facilities and logical access to computers/information systems as required
- ✓ Treat your PIV or Non-PIV card with the same care you would give other identification credentials, such as your driver's license, credit card or social security card
- ✓ Keep your PIV or Non-PIV card with you at all times and display it above the waist when not in use
- ✓ Report a stolen or missing credential:
  - Within 24 hours or the next business day, report it to your local badging office
  - Coordinate with your PIV Sponsor to have PIV/Non-PIV card reissued
- ✓ Use your PIV or Non-PIV card to logon to the VA network
- ✓ Make an appointment with your badging office six weeks ahead of the expiration date to ensure you get your credential renewed in time
- ✓ Surrender your PIV or Non-PIV card when you resign, retire or end your affiliation with VA

## DON'T

- ✗ Don't write down your PIN anywhere
- ✗ Don't share your credential or PIN with anyone
- ✗ Don't alter the credential in any way (do not scratch it, bend it, make holes in it or attach anything to it)
- ✗ Don't wear your PIV or Non-PIV card in an MRI room or near MRI or similar magnetic devices
- ✗ Don't keep your PIV or Non-PIV card in anything other than the VA-issued electromagnetically opaque card holder
- ✗ Don't leave your credential unattended

*"The price of freedom is eternal vigilance."*  
- Thomas Jefferson

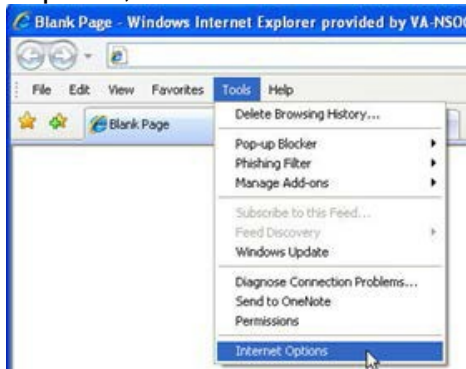


## Attachment 5

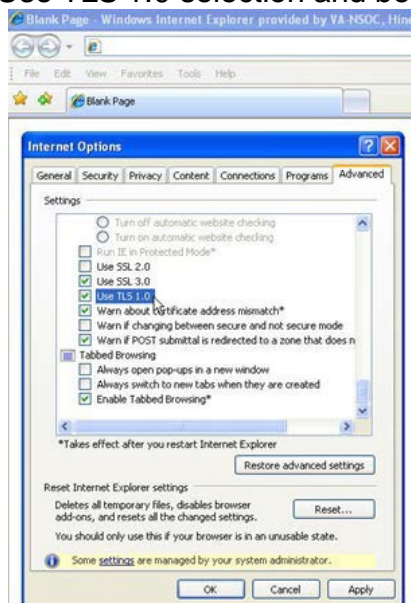
### LOGGING INTO VPN/CAG (FOR REMOTE USERS)

These instructions are for individuals trying to log into the Citrix Access Gateway (CAG) with access to any computer device (*i.e. Laptop, Desktop*). Depending on the speed of your PC and Internet connection, this installation may take several minutes.

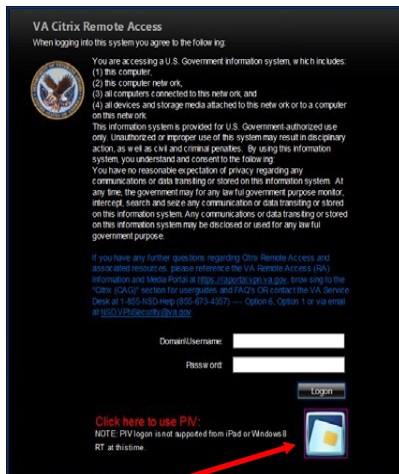
1. Verify that Transport Layer Security 1.0 is enabled on your browser. For Internet Explorer, select the Tools menu item and click **Internet Options**.



2. From the Internet Options window, select the advanced tab. Scroll down to the Use TLS 1.0 selection and be sure it is selected. Click OK and close the browser



3. Open Internet browser again and access CAG at the following URL: <https://citrixaccess.va.gov>



4. Click on the card reader icon.
5. If a certificate selection pop-up window opens, select the internal PIV Authentication certificate that contains your name.

To figure out which certificate is your internal PIV Authentication certificate: Hover the mouse cursor over the certificate to display the certificate description. Check the description for the certificate is internal PIV Authentication.

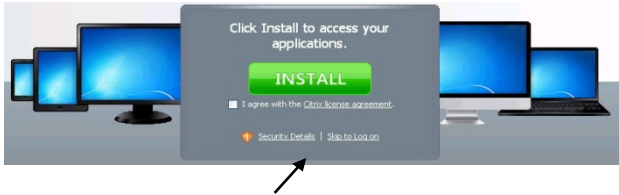


(The certificate has numbers after it.)

6. Enter your PIV card PIN in the login box that appears. Click the **OK** button.

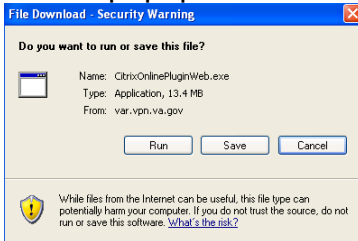


7. If this is your first time using Citrix, you may be given option to install the latest Citrix client. Simply check to agree with the license agreement and click **INSTALL**



**Note: If you have previously installed this application, then click (Skip to Log in).**

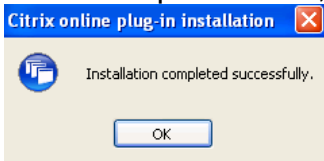
8. On the popup screen below, click **RUN** to start downloading the Citrix client.



9. Once downloading the client is complete, you'll need to click **RUN** again to install the client.



10. After a couple minutes, the client installation will finish. Please click **OK**.



**NOTE:** You may get a pop up window that asks “Add Account”. If you get this message, do not input anything into the window. Click on **OK** and bypass the window.

11. Once the installation is completed Citrix will continue logging you on and redirect you to Citrix home screen showing the most commonly used applications such as: Outlook, CPRS, Internet Explorer or Excel as shown below.

To launch an application, simply “**single click**” on the icon

**Note.** Depending on your access, your Citrix home screen might have different applications listed. If an application is not working properly or fails to launch, it could mean that your previous sessions might not have been logged off properly.

12. To access the VBA App Desktop, Select Desktop tab from screen shot above, then follow steps below.



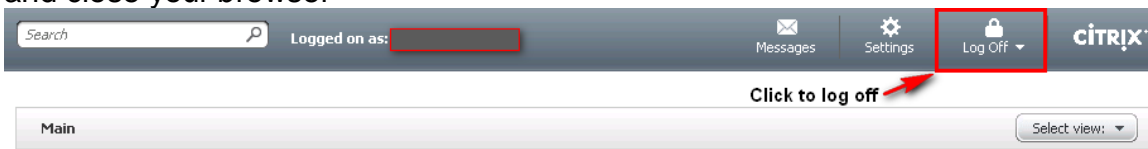
13. Double click on monitor icon to begin login process.



Click OK

**Note: Depending on the speed of your PC and Internet connection, this may take several minutes.**

14. When done using Citrix, make sure your session is released by clicking on **LOG OFF** and close your browser



**Warning:** You must click on **LOG OFF** before closing the internet browser. Without doing so, you might end up having multiple sessions on different servers and they can get stuck or corrupted and prevent applications from working properly. Logging off properly will ensure that all previous sessions, including the corrupted & idle sessions get released so that the next time you use Citrix, all applications will run smoothly.

**Support info.** For all issues related to National Citrix Access Gateway, contact the help desk at: 1-855-673-4357. Press Option “6”, then Option “1.”

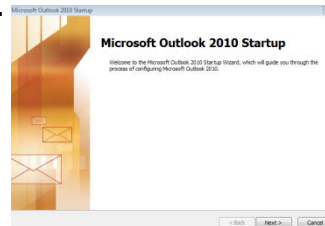
## Attachment 6

### LOADING OUTLOOK AND CONFIGURING PIV CARD

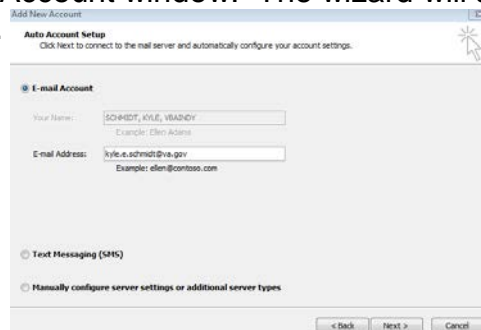
Before configuring your PIV card you will need to open Microsoft Outlook and run the setup wizard to load your Outlook account. To load Outlook on your computer, perform the following steps:

#### Loading Outlook

1. From the start menu, find Microsoft Outlook and double click to open.
2. The Startup window will appear, click **NEXT**



3. Account Configuration Window: Select **YES** and then **NEXT**
4. Add New Account window: The wizard will automatically load your email address, select **NEXT**.

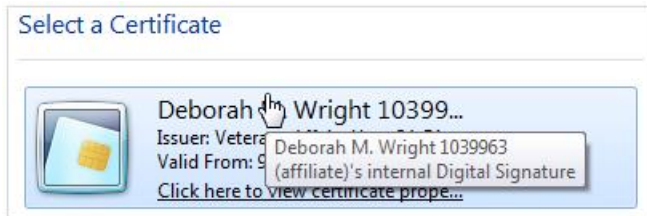


5. Outlook will then configure your email settings. This may take several minutes to accomplish, please be patient. When complete the NEXT button will be highlighted, select **NEXT**.
6. Once all your settings have been established by Outlook the Finish button will be highlighted, select **FINISH**.
7. Outlook will open and begin loading all of your settings. This could take a few minutes, before you are able to use Outlook. Once it is complete, move to the next steps to configure your PIV card.



## Configuring Outlook: Publishing PIV Certs to the Global Address List

1. Insert your PIV card into the card reader. This may be located on your keyboard or thru an attached USB device.
2. In Outlook, select the **File Tab**. The Microsoft Office Backstage view appears. Under Help, click **Options**.
3. In the Options Dialog, click **Trust Center**, and then click **Trust Center Settings**.
4. Select **E-mail Security** from left column and click on the **Settings** button to display the Change Security Settings window.
5. Confirm that the **Secure Settings Name** displays My **S/MIME Settings** and that the Secure Message Format displays **S/MIME**.
6. To the right of Signing Certificate, click **Choose**.
7. A new window entitled Select Certificate will open. Select your PIV signing certificate. PIV certificates have your name followed by a series of numbers. Hover over your name and select the certificate with **Digital Signature** in the tool-tip/pop-up. Click **OK**.



8. You will then be returned to the Change the Security Setting screen.
9. Repeat the process for your **Encryption Certificate** by clicking **Choose** to the right of the Encryption Certificate box. Hover over your name and select the certificate with **Key Management** in the tool-tip/pop-up. Click **OK**.



10. A window entitled Select Certificate will pop up. Confirm your PIV certificate is selected. Click **OK**.
11. You will return to the Change the Security Setting screen. Click **OK**. The window closes and you will be returned to the Trust Center screen, under the E-mail Security window.
12. Click **Publish to GAL**.
13. Outlook will indicate you are about to publish to the **Global Address List (GAL)**. Click **OK**.
14. When publishing to the GAL, Outlook will access your PIV card. Enter the PIN associated with your PIV card and Click **OK**.
15. Once the certificate is published Outlook will show a success message. Click **OK**; your certificates are published to the GAL.
16. You can now close any remaining windows and resume using Outlook.


For any issues call NSD Specialty 855-673-4357 Option 6, then option 2 or 3.

## Attachment 7

### LOGGING INTO SHARE AND VBMS

Now that you have logged into the VA network and configured your PIV card, you are able to log into VA Applications, such as SHARE and VBMS. Please follow the instructions below to log in for the first time.


**Logging into SHARE:** You must first log into SHARE before any other application to update your password.

1. Select the Microsoft Start icon 
2. Select **All Programs**
3. Select **VBAPPS**
4. Select **SHARE T11** (The SHARE log in window appears)



5. For initial log in, your temporary password is the FIRST 8 CHARACTERS OF YOUR LAN USERID (in all caps). You will be prompted to change your password. Create an 8-digit password.
6. Log out of SHARE

### **Logging into VBMS:**

1. Select the Microsoft Start icon 
2. Select **All Programs**
3. Select **VBAPPS**
4. Open the VBMS folder; then select **VBMS**

## Attachment 8

### USEFUL INFORMATION AND TRAINING LINKS

Now that you have logged into the VA network you have access to certain VA Applications. Below are links that you may use to learn the functions of the applications.

Veterans Benefits Management System (VBMS):

[VBMS VSO Corner](#)

[VBMS Minute Videos](#)

[VBMS Stakeholder Toolkit](#)

[VBMS Job Aid: eFolder Fundamentals](#)

[VBMS Job Aid: Searching for a Veteran Profile](#)

[VBMS Job Aid: Viewing Intent to File Information in VBMS](#)

COVERS:

[COVERS Online User Guide](#)

VSO VOCALS:

[Part 1 – Logging On](#)

[Part 2 – Regional Office Screen](#)

[Part 7 – VACOLS Codes](#)

Virtual VA:

[Virtual VA User Guide](#)

Stakeholder Enterprise Portal:

[SEP Home Page](#)

[SEP User Guide](#)

[SEP Frequently Asked Questions](#)

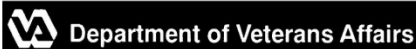
Enclosure: (Required Forms)

The following forms are required to be submitted to initiate a background check and to request a PIV badge. Please complete as requested in the Initial Access Checklist, step 6, and fax them to **(215) 713-1112**.

-VA 0711 (see page 29-31)

-VBA 20-0344 (see page 32-33)

-Declaration for Federal Background Investigation for Affiliates and Volunteers (see page 34)



## REQUEST FOR PERSONAL IDENTITY VERIFICATION CARD

**PRIVACY ACT STATEMENT:** VA is authorized to ask for the information requested on this form by Homeland Security Presidential Directive (HSPD)-12, and 31 USC 7701. The information and biometrics collected, collected as part of the Federal identity-proofing program under HSPD-12 are used to verify the personal identity of VA applicants for employment, employees, contractors, and affiliates (such as students, WOC employees, and others) prior to issuing a Department identification credential. The credentials themselves are to be used to authenticate electronic access requests from VA employees, contractors, and affiliates issued a Department identification credential to gain access to VA facilities and networks (where available) through digital access control systems, as well as to other federal government agency facilities and systems where permitted by law. The information collected on this form is protected by the Privacy Act, 5 USC Section 552(a) and maintained under the authority of 38 USC Section 501 and 38 USC Sections 901-905 in VA system of records "Police and Security Records-VA (103VA07B)". VA may make a "routine use" disclosure of the information in this system of records for the routine uses listed in this system of records, including: civil or criminal law enforcement, constituent congressional communications initiated at your request, litigation or administrative proceedings in which the United States is a party or has an interest, the administration of VA programs, verification of identity and status, and personnel administration by Federal agencies. Failure to provide all of the requested information may result in VA being unable to process your request for a Personal Identity Verification Card, or denial of issuance of a Personal Identity Verification Card. If you do not have a Personal Identity Verification Card, you may not be granted access to VA facilities or networks, which could have an adverse impact on your application to become, or status as, a VA employee, contractor or affiliate where such access is required to perform your assigned duties or responsibilities.

**PAPERWORK REDUCTION ACT NOTICE:** The public reporting burden is approximately 5 minutes including time to review instruction, find the information, and complete this form. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to the VA Clearance Officer (005E3), 810 Vermont Avenue, Washington, DC 20420.

### SECTION I - APPLICANT INFORMATION

#### APPLICANT INFORMATION (Completed by Applicant)

1. LEGAL NAME OF APPLICANT (Insert last, first, middle and suffix name)		2. NICKNAME TO BE USED FOR APPLICANT (Insert last name and first name, if applicable)	
3. DATE OF BIRTH (MM/DD/YYYY)	4. SOCIAL SECURITY NO.	5. HOME PHONE NUMBER (Include Area Code) (Optional)	
6. HOME E-MAIL ADDRESS (Optional)		7. HOME ADDRESS	
8. SIGNATURE OF APPLICANT		9. DATE SIGNED	

### SECTION II - SPONSOR VERIFICATION (Completed by Sponsor)

#### PART A - APPLICANT EMPLOYMENT INFORMATION (Completed by Sponsor)

1. NAME AND ADDRESS OF FACILITY OR ASSIGNED DUTY STATION		2. NAME OF SPONSORING DEPARTMENT, SERVICE, OR SECTION, AND MAIL ROUTING SYMBOL	
		3. CREDENTIALS/ORGANIZATIONAL TITLE (AKA Position/Job Title)	4. COST CTR.
		5. WORK PHONE NUMBER (If applicable)	6. WORK E-MAIL ADDRESS

#### PART B - TYPE OF REQUEST AND EMPLOYMENT STATUS (Completed by Sponsor)

1. TYPE OF REQUEST <input type="checkbox"/> NEW ID <input type="checkbox"/> RENEWAL <input type="checkbox"/> REPLACEMENT ID (Damaged/Lost) <input type="checkbox"/> CHANGE LEVEL OF ACCESS			
2. TYPE OF CARD <input type="checkbox"/> PERSONAL IDENTITY VERIFICATION (PIV) <input type="checkbox"/> VA (NON-PIV)		3. TYPE OF ACCESS <input type="checkbox"/> LOGICAL ACCESS _____ (Domain) <input type="checkbox"/> PHYSICAL ACCESS (Complete Part D)	
4. EMPLOYMENT STATUS <input type="checkbox"/> VA EMPLOYEE <input type="checkbox"/> CONTRACTOR <input type="checkbox"/> AFFILIATE (Specify) <input type="checkbox"/> TEMPORARY VA EMPLOYMENT			

#### PART C - PHYSICAL SECURITY ACCESS DATA (Completed by Sponsor)

1. SPECIAL SECURITY ACCESS REQUIRED  <input type="checkbox"/> YES (If "YES," Specify in Item2) <input type="checkbox"/> NO	2. SPECIFY LOCATION OF SPECIAL SECURITY (i.e. tower, bldg. no., etc.)  	3. IS APPLICANT A KEY EMERGENCY RESPONDER, CRITICAL EMPLOYEE, OR NEITHER? <input type="checkbox"/> EMERGENCY RESPONDER <input type="checkbox"/> CRITICAL EMPLOYEE <input type="checkbox"/> NEITHER
--	---	--

#### PART D - TYPE OF BACKGROUND INVESTIGATION FOR POSITION (Completed by Sponsor)

TYPE OF BACKGROUND INVESTIGATION FOR POSITION <input type="checkbox"/> SAC <input type="checkbox"/> NACI <input type="checkbox"/> SECRET <input type="checkbox"/> TOP SECRET <input type="checkbox"/> OTHER (Specify)				
--	--	--	--	--

#### PART E - CONTRACTORS, AFFILIATES, AND TEMPORARY EMPLOYMENT INFORMATION (Completed by Sponsor)

1. EMPLOYMENT EXPIRATION DATE /CONTRACT END DATE (MM/DD/YYYY)(For Contractors, Affiliates, and Temporary Employment)  		2. NAME OF FIRM OR COMPANY (If applicable)	
3. NAME OF CONTRACTING OFFICER TECH. REPR. (If applicable)		4. NAME OF RESPONSIBLE VA ORGANIZATION	5. MAIL ROUTING SYM.

<b>PART F - SPONSOR AUTHORIZATION AND CERTIFICATION (Completed by Sponsor)</b>									
<b>CERTIFICATION:</b> I Certify under penalty of perjury that the information in Section II is true and correct.									
1. NAME OF SPONSOR				2. SPONSOR CREDENTIALS/ORGANIZATIONAL TITLE					
3. CERTIFICATE NUMBER <i>(Issued by PCI Manager or Registrar)</i>				4. SIGNATURE OF SPONSOR				5. DATE SIGNED <i>(MM/DD/YYYY)</i>	
6. WORK ADDRESS				7. NAME OF SPONSOR'S DEPARTMENT, SERVICE, OR SECTION					
				8. WORK PHONE NUMBER <i>(Include Area Code)</i>					
				9. WORK E-MAIL ADDRESS					
<b>SECTION III - APPLICANT IDENTITY VERIFICATION (Completed by Registrar)</b>									
<b>INSTRUCTIONS:</b> To be completed and signed by Registrar at the time of proofing. Review Section I - Applicant Information, and Section II - Sponsor Verification, assuring that information has been filled out correctly and signed accordingly. The identification must follow these guidelines: <ul style="list-style-type: none"> <li>● Applicant must present two (2) forms of identification from the Accepted Identification Documentation List.</li> <li>● The names on the identification must match exactly (If one ID has a full middle name, and the other has a middle initial, then the initial must match).</li> <li>● One State or Federal ID must contain a photograph. ● Both IDs must be original documents. ● Both IDs must be currently valid, not expired.</li> <li>● Verify that the applicant has background information on file. If no evidence of a SAC exists, then capture fingerprint data and process accordingly.</li> </ul>									
<b>PART A - BACKGROUND CHECK</b>									
1. TYPE OF BACKGROUND CHECK									
1A. DATE INITIATED BACKGROUND CHECK <i>(MM/DD/YYYY)</i>		SAC <i>(Fingerprint Check)</i>			NACI		OTHER <i>(Specify)</i>		
1B. DATE ADJUDICATED BACKGROUND CHECK <i>(MM/DD/YYYY)</i>									
2. FINGERPRINTS CAPTURE REQUIRED? <input type="checkbox"/> YES <input type="checkbox"/> NO <i>(If "NO," proceed to Part B)</i>		3. SEX	4. RACE	5. HEIGHT	6. WEIGHT	7. EYES	8. HAIR	9. PLACE OF BIRTH	
10. NOTICABLE SCARS AND TATTOOS									
<b>PART B - PHOTOGRAPHIC IDENTIFICATION NUMBER 1</b>									
1. EXACT NAME LISTED ON PHOTO ID		2. DOCUMENT IDENTIFICATION NUMBER				3. EXPIRATION DATE <i>(MM/DD/YYYY)</i>			
4. DOCUMENT TYPE		5. ISSUANCE DATE <i>(MM/DD/YYYY)</i>				6. ISSUING AUTHORITY			
<b>PART C - IDENTIFICATION NUMBER 2</b>									
1. EXACT NAME LISTED ON ID		2. DOCUMENT IDENTIFICATION NUMBER				3. EXPIRATION DATE <i>(MM/DD/YYYY)</i>			
4. DOCUMENT TYPE		5. ISSUANCE DATE <i>(MM/DD/YYYY)</i>				6. ISSUING AUTHORITY			
<b>PART D - REGISTRAR INFORMATION AND SIGNATURE</b>									
1. WORK ADDRESS				2. PRINTED NAME OF REGISTRAR					
				3. NAME OF DEPARTMENT, SERVICE, OR SECTION					
				4. WORK PHONE NUMBER <i>(Include Area Code)</i>				5. WORK E-MAIL ADDRESS	
6. DATE APPLICANT INITIATED BACKGROUND INVESTIGATION				7. APPLICANT'S REQUEST FOR PERSONAL IDENTITY VERIFICATION CARD <b>ACTION TAKEN:</b> <input type="checkbox"/> APPROVED <input type="checkbox"/> DENIED					
<b>CERTIFICATION:</b> I certify that under penalty of perjury that I have examined the documents presented by the above named person, and that the above listed documents appear to be genuine and to relate to the person named.									
8. SIGNATURE OF REGISTRAR						9. DATE SIGNED <i>(MM/DD/YYYY)</i>			

<b>SECTION IV - PERSONAL IDENTITY VERIFICATION CARD ACCEPTANCE</b>		
<b>PART A - CARD INFORMATION (Completed by Issuer)</b>		
1. NEW PIV CREDENTIAL SERIAL NUMBER	2. OLD ACCESS ID CARD NUMBER	3. EXPIRATION DATE (MM/DD/YYYY)
<b>PART B - PERSONAL IDENTITY VERIFICATION CARD ACCEPTANCE (Completed by Applicant)</b>		
<b>ACKNOWLEDGEMENT:</b> I acknowledge receiving my identity credential and will comply with the following obligations: <ul style="list-style-type: none"> <li>● I have been provided training on the responsibilities associated with receipt of this Personal Identity Verification Card.</li> <li>● I will use my Personal Identity Verification card in accordance with the training I have been provided.</li> </ul>		
<b>CERTIFICATION:</b> I certify that I have read and agree to the above statements and that I have received my card.		
1. PRINTED NAME OF APPLICANT	2. APPLICANT SIGNATURE OF ACCEPTANCE	3. DATE SIGNED (MM/DD/YYYY)
<b>PART C - PUBLIC KEY INFORMATION (PKI) CERTIFICATE ACCEPTANCE (Completed by Applicant)</b>		
<b>AUTHORIZATION STATEMENT</b> You have been authorized to receive one or more private and public key pairs and associated certificates. A private key enables you to digitally sign documents and messages and identify yourself to gain access to information systems and facilities. You may have another private key to decrypt data such as encrypted messages. People and electronic systems inside and outside VA will use public keys associated with your private keys to verify your digital signature, or to verify your identity when you attempt to authenticate to systems, or to encrypt data sent to you. The certificates and private keys will be issued on a token, for example your Personal Identity Verification Card. The token and the certificates and private keys on your token are government property. Users are authorized to use the certificates within VA, as well as while conducting business with other Federal, state, and Local Government agencies.		
<b>ACKNOWLEDGEMENT OF RESPONSIBILITIES</b> <ul style="list-style-type: none"> <li>● I represent and warrant that the information provided in application for this certificate is accurate, current, and complete. If this information changes, I will notify my Registrar of the changes;</li> <li>● I will use my certificate(s) and private key(s) for official purposes only;</li> <li>● I will comply with the Certificate Practices Statement for selecting a Personal Identification Number (PIN) or other required method for controlling access to my private keys and will not disclose same to anyone, leave it where it might be observed, nor write it on the token itself;</li> <li>● I understand that digital signatures applied using my digital certificates carry the same legal obligation as my physically signing the document;</li> <li>● I understand that if I receive key management (encryption/decryption) key pairs on my token, copies of the private decryption keys have been provided to the key recovery database in case they need to be recovered; and</li> <li>● I will report any compromise (e.g., loss, suspected or known unauthorized use, misplacement, etc.) of my PIN or token to my supervisor, security officer, Certification Authority (CA), or a Registrar, immediately.</li> </ul>		
<b>LIABILITY</b> I will have no claim against VA arising from use of the PKI certificates, the key recovery process, or a Certification Authority's (CA) determination to terminate or revoke a certificate. VA is not liable for any losses, including direct or indirect, incidental, consequential, special, or punitive damages, arising out of or relating to any certificate issued by a VA CA.		
<b>GOVERNMENT LAW</b> VA Public Key Certificates shall be governed by the laws of the United States of America.		
<b>CERTIFICATION:</b> I certify that I have read and agree to the above statements and that I have received my PKI certificate(s).		
1. FULL LEGAL NAME OF APPLICANT	2. SIGNATURE OF ACCEPTANCE	3. DATE SIGNED (MM/DD/YYYY)
<b>SECTION V - ISSUER (Completed by Issuer)</b>		
1. WORK ADDRESS	2. PRINTED NAME OF ISSUER	
	3. NAME OF DEPARTMENT, SERVICE, OR SECTION	
	4. WORK PHONE NUMBER (Include Area Code)	5. WORK E-MAIL ADDRESS
<b>CERTIFICATION:</b> I certify under penalty of perjury, that I have monitored the identity verification of the person above in accordance with applicable identity proofing processes and have witnessed that person sign this form.		
6. SIGNATURE OF ISSUER	7. DATE SIGNED (MM/DD/YYYY)	





Department of Veterans Affairs

**ANNUAL CERTIFICATION OF VETERAN STATUS AND VETERAN-RELATIVES**

**Privacy Act Notice:** The VA will not disclose information collected on this form to any source other than what has been authorized under the Privacy Act of 1974 or Title 38, Code of Federal Regulations 1.576 for routine uses (i.e., civil or criminal law enforcement, congressional communications, epidemiological or research studies, the collection of money owed to the United States, litigation in which the United States is a party or has an interest, the administration of VA programs and delivery of VA benefits, verification of identity and status, and personnel administration) as identified in the VA system of records, 58VA21/22, Compensation, Pension, Education and Rehabilitation Records - VA, published in the Federal Register. Your obligation to respond is mandatory. Giving us your and your veteran relatives' SSN account information is mandatory. Any persons, including dependents and beneficiaries, who apply for or receive VA Compensation and Pension benefits are required to provide their SSN under Title 38 USC 5101(c)(1). The VA will not deny an individual benefits for refusing to provide his or her SSN unless the disclosure of the SSN is required by a Federal Statute of law in effect prior to January 1, 1975, and still in effect. The responses you submit are considered confidential (38 U.S.C. 5701). Information submitted is subject to verification through computer matching programs with other agencies.

**Respondent Burden:** We need this information to identify the benefit records VA maintains for you and your relatives in order to insure the security and confidentiality of the records (5 U.S.C. 552a(e)(10)). Title 38, United States Code, allows us to ask for this information. We estimate that you will need an average of 25 minutes to review the instructions, find the information, and complete this form. VA cannot conduct or sponsor a collection of information unless a valid OMB control number is displayed. You are not required to respond to a collection of information if this number is not displayed. Valid OMB control numbers can be located on the OMB Internet Page at [www.reginfo.gov/public/do/PRAMain](http://www.reginfo.gov/public/do/PRAMain). If desired, you can call 1-800-827-1000 and give your comments or ask for mailing information on where to send your comments.

**SECTION I - EMPLOYEE INFORMATION**

1. EMPLOYEE'S LAST NAME, FIRST NAME, MIDDLE INITIAL	2. EMPLOYEE'S SOCIAL SECURITY NUMBER
3. EMPLOYEE'S DATE OF BIRTH (MONTH, DAY, YEAR)	4. REGIONAL OFFICE OF EMPLOYMENT
5. HAVE YOU EVER APPLIED FOR OR RECEIVED BENEFITS FROM THE DEPARTMENT OF VETERANS AFFAIRS (Either as a veteran or a veteran's dependent)? <input type="checkbox"/> YES <input type="checkbox"/> NO	
6. HAVE YOU EVER SERVED ON ACTIVE DUTY IN THE U.S. MILITARY? <input type="checkbox"/> YES <input type="checkbox"/> NO	

**Note:** If your answer is "no" to **both** Items 5 and 6 above, skip Section II and proceed to Section III on the reverse to complete the remainder of the form. If your answer is "yes" to either or both items, please complete the entire form including Items 7 through 14 below. If you are a veteran, provide the information requested in Items 7 through 14 relative to your military status and VA claims records. If you are a veteran's dependent, provide the requested information for the veteran on whom your benefits eligibility is based.

**SECTION II - VETERAN EMPLOYEE/VETERAN'S DEPENDENT INFORMATION**

7. VETERAN'S FULL NAME AS USED IN MILITARY SERVICE (Last, First, Middle)		
8. YOUR RELATIONSHIP TO VETERAN <input type="checkbox"/> SELF <input type="checkbox"/> SPOUSE <input type="checkbox"/> CHILD <input type="checkbox"/> PARENT		
9. VETERAN'S MILITARY SERVICE NUMBER		
10. VETERAN'S SOCIAL SECURITY NUMBER	11. VETERAN'S DATE OF BIRTH (MONTH, DAY, YEAR)	
12. INSURANCE FILE NUMBER (If applicable)		
13. CLAIMS FILE NUMBER (If applicable)		
14. VA BENEFITS APPLIED FOR (Check all boxes that apply)		
<input type="checkbox"/> NONE	<input type="checkbox"/> TOTAL OR TOTAL AND PERMANENT DISABILITY (USGLI)	<input type="checkbox"/> TOTAL DISABILITY (NSLI)
<input type="checkbox"/> DISABILITY COMPENSATION	<input type="checkbox"/> PENSION	<input type="checkbox"/> RETIREMENT PAY
<input type="checkbox"/> VOCATIONAL REHABILITATION	<input type="checkbox"/> EDUCATION OR TRAINING	<input type="checkbox"/> LOAN GUARANTY
<input type="checkbox"/> HOSPITAL OR DOMICILIARY CARE	<input type="checkbox"/> OUTPATIENT TREATMENT	<input type="checkbox"/> OTHER (Specify below)



SECTION III - INFORMATION ABOUT YOUR RELATIVES WHO ARE VETERANS AND/OR VA BENEFICIARIES	
Note: List all relatives (spouse, child, parent, sibling) who are veterans or who have applied for or are receiving benefits as a veteran's dependent. If assistance is needed in obtaining military service numbers and/or claims numbers, please see your station's IT Security Officer. Check Item 18 "Additional Information" and attach a separate sheet if more space is needed.	
15. RELATIVE INFORMATION - FIRST	
A. RELATIVE'S LAST NAME, FIRST NAME, MIDDLE NAME ▶	
B. RELATIONSHIP TO YOU ▶	<input type="checkbox"/> SPOUSE <input type="checkbox"/> CHILD <input type="checkbox"/> PARENT <input type="checkbox"/> SIBLING
C. VETERAN'S FULL NAME AS USED IN MILITARY SERVICE (LAST, FIRST, MIDDLE) ▶	
D. VETERAN'S SOCIAL SECURITY NUMBER ▶	
E. VETERAN'S MILITARY SERVICE NUMBER ▶	
F. INSURANCE FILE NUMBER ▶	
G. CLAIMS FILE NUMBER ▶	
H. VETERAN'S BIRTHDATE (MONTH, DAY, YEAR) ▶	
16. RELATIVE INFORMATION - SECOND	
A. RELATIVE'S LAST NAME, FIRST NAME, MIDDLE NAME ▶	
B. RELATIONSHIP TO YOU ▶	<input type="checkbox"/> SPOUSE <input type="checkbox"/> CHILD <input type="checkbox"/> PARENT <input type="checkbox"/> SIBLING
C. VETERAN'S FULL NAME AS USED IN MILITARY SERVICE (LAST, FIRST, MIDDLE) ▶	
D. VETERAN'S SOCIAL SECURITY NUMBER ▶	
E. VETERAN'S MILITARY SERVICE NUMBER ▶	
F. INSURANCE FILE NUMBER ▶	
G. CLAIMS FILE NUMBER ▶	
H. VETERAN'S BIRTHDATE (MONTH, DAY, YEAR) ▶	
17. RELATIVE INFORMATION - THIRD	
A. RELATIVE'S LAST NAME, FIRST NAME, MIDDLE NAME ▶	
B. RELATIONSHIP TO YOU ▶	<input type="checkbox"/> SPOUSE <input type="checkbox"/> CHILD <input type="checkbox"/> PARENT <input type="checkbox"/> SIBLING
C. VETERAN'S FULL NAME AS USED IN MILITARY SERVICE (LAST, FIRST, MIDDLE) ▶	
D. VETERAN'S SOCIAL SECURITY NUMBER ▶	
E. VETERAN'S MILITARY SERVICE NUMBER ▶	
F. INSURANCE FILE NUMBER ▶	
G. CLAIMS FILE NUMBER ▶	
H. VETERAN'S BIRTHDATE (MONTH, DAY, YEAR) ▶	
18. ADDITIONAL INFORMATION	
<input type="checkbox"/> Please check if additional relatives are identified on an attachment to this form.	
I certify that the above information is correct and complete to the best of my knowledge.	
19. SIGNATURE OF EMPLOYEE (Do NOT Print)	20. DATE SIGNED
<div style="border: 1px solid black; height: 20px; width: 100%;"></div>	

## Declaration for Federal Background Investigation for Affiliates and Volunteers

GENERAL INFORMATION	
FULL NAME	
SOCIAL SECURITY	
PLACE OF BIRTH	
ARE YOU A U.S. CITIZEN?	
DATE OF BIRTH	
OTHER NAMES EVER USED <i>(For example, maiden name, nickname, etc)</i>	
PHONE NUMBER (DAY)	PHONE NUMBER (NIGHT)
SELECTIVE SERVICE REGISTRATION	
ARE YOU A MALE BORN AFTER DECEMBER 31, 1959?	
HAVE YOU REGISTERED WITH THE SELECTIVE SERVICE SYSTEM? <i>(If "NO," describe reason in continuation space)</i>	
MILITARY SERVICE	
HAVE YOU EVER SERVED IN THE UNITED STATES MILITARY? <i>(If "YES," provide information below)</i>	
BRANCH	BRANCH
FROM (MM/DD/YYYY)	FROM (MM/DD/YYYY)
TO (MM/DD/YYYY)	TO (MM/DD/YYYY)
TYPE OF DISCHARGE	TYPE OF DISCHARGE
BACKGROUND INFORMATION	
DURING THE LAST 7 YEARS, HAVE YOU BEEN CONVICTED, BEEN IMPRISONED, BEEN ON PROBATION, OR BEEN ON PAROLE? <i>(Includes felonies, firearms or explosive violations, misdemeanors, and all other offenses.) If "YES," use Continuation Space to provide the date, explanation of the violation, place of occurrence, and the name and address of the police department or court involved.</i>	
HAVE YOU BEEN CONVICTED BY A MILITARY COURT-MARTIAL IN THE PAST 7 YEARS? <i>(If no military service, answer "NO.") If "YES," use Continuation Space to provide the date, explanation of the violation, place of occurrence, and the name and address of the military authority or court involved.</i>	
ARE YOU CURRENTLY UNDER CHARGES FOR ANY VIOLATION OF LAW? <i>If "YES," use Continuation Space to provide the date, explanation of the violation, place of occurrence, and the name and address of the police department or court involved.</i>	
DURING THE LAST 5 YEARS, HAVE YOU BEEN FIRED FROM ANY JOB FOR ANY REASON, DID YOU QUIT AFTER BEING TOLD THAT YOU WOULD BE FIRED, DID YOU LEAVE ANY JOB BY MUTUAL AGREEMENT BECAUSE OF SPECIFIC PROBLEMS, OR WERE YOU DEBARRED FROM FEDERAL EMPLOYMENT BY THE OFFICE OF PERSONNEL MANAGEMENT OR ANY OTHER FEDERAL AGENCY? <i>If "YES," use Continuation Space to provide the date, an explanation of the problem, reason for leaving, and the employer's name and address.</i>	
ARE YOU DELINQUENT ON ANY FEDERAL DEBT? <i>(Includes delinquencies arising from Federal taxes, loans, overpayment of benefits, and other debts to the U.S. Government, plus defaults of Federally guaranteed or insured loans such as student and home mortgage loans.) If "YES," use Continuation Space to provide the type, length, and amount of the delinquency or default, and steps that you are taking to correct the error or repay the debt.</i>	

<p><b>DO ANY OF YOUR RELATIVES WORK FOR THE AGENCY OR GOVERNMENTAL ORGANIZATION TO WHICH YOU ARE SUBMITTING THIS FORM?</b> (Includes: father, mother, husband, wife, son, daughter, brother, sister, uncle, aunt, first cousin, nephew, niece, father-in-law, mother-in-law, son-in-law, daughter-in-law, brother-in-law, sister-in-law, stepfather, stepmother, stepson, stepdaughter, stepbrother, stepsister, half-brother, and half-sister.) <i>If "YES," use Continuation Space to provide the relative's name, relationship, and the department, agency, or branch of the Armed Forces for which your relative works.</i></p>	
<p align="center"><b>CONTINUATION SPACE</b></p>	
<p align="center"><b>CERTIFICATION</b></p>	
<p><b>I certify</b> that, to the best of my knowledge and belief, all of the information on and attached to this document, including any attached materials, is true, correct, complete, and made in good faith. <b>I understand that a false or fraudulent answer to any question or item on any part of this document or its attachments may be grounds for an unfavorable result of the system access I am seeking and may be punishable by fine or imprisonment.</b> I understand that any information I give may be investigated for purposes of establishing access to Federal government systems as allowed by law or Presidential order. <b>I consent</b> to the release of information about my ability and fitness for this access by employers, schools, law enforcement agencies, and other individuals and organizations to investigators, personnel specialists, and other authorized employees or representatives of the Federal Government. <b>I understand</b> that for financing or lending institutions, medical institutions, hospitals, health care professionals, and some other sources of information, a separate specific release may be needed, and I may be contacted for such a release at a later date.</p>	
<p><b>SIGNATURE</b> <i>(Sign in ink)</i></p>	
<p><b>DATE</b></p>	