Memorandum of Understanding

The following constitutes an Agreement between the Department of Veterans Affairs (VA) and the National Federation of Federal Employees (NFFE) on Mandatory Use of Personal Identity Verification (PIV)/Multifactor Authentication for Access to VA Information Systems.

1. Bargaining unit employees shall not be adversely affected by the implementation of the PIV Multifactor Authentication for access to VA Information Systems as it relates to employees job performance.

2. If a PIV card is lost, stolen or irrevocably destroyed, the employee will avail themselves of a local procedure for interim access. Replacement will be done as soon as possible. In any event, the replacement card will be at no cost to the employee.

3. If or when bargaining unit employees require a replacement PIV badge due to damage, defect, loss or expiration of their current badge, the employee will be kept in a duty status, have access to their office, work space, computer system, and be afforded duty time to apply and or reactivate the PIV card. Temporary user ID and Password for network access will be obtained through contact with the National Help Desk.

4. The employer will provide a protective shield and card holder for all employees. The employer will provide a lanyard to have card attach in the most secure manner.

5. The parties agree to follow VA Handbook 0735 as it pertains to the use of PIV badges for Federal employees.

6. Employees agree to report immediately the loss of their PIV card to an appropriate Agency official.

7. Bargaining unit employees who are assigned in remote locations or Outpatient clinics will generally be issued a PIV cards at their worksites. If a bargaining unit employee is required to travel to another site to obtain a PIV card, the employee will be permitted to be on duty time and follow the Joint Travel Regulation (JTR).

8. Currently, VA Handbook 0735, Section 7, PIV Privacy Guidelines does not provide for the use of PIV badges for timekeeping purposes or for tracking of employee movement [or location]. With the implementation of the use of PIV badges for network access, the Parties agree there is no intent to do so at this time, however, should this change, the Department will notify the Union and meet all bargaining obligations prior to implementing the change.

9. Bargaining unit employees will be informed of their designated sponsors for PIV cards.

10. Bargaining unit employees will be provided a Frequently Asked Questions/Fact Sheet outlining the process for utilizing their PIV badge for network access.

11. Employees may select a Personal Identification Number (PIN) of their choice for the Personal Identification Verification (PIV) card. Employees may choose any number meeting the minimal required digits.

12. Management will notify the NFFE VA Council President prior to any changes in VA Handbook 0735 and bargain as appropriate.

13. In accordance with Article 8, Section 2(E) of the VA/NFFE Master Agreement NFFE Locals may bargain over the implementation of the PIV Multifactor Authentication for access to VA Information Systems, so long as there is no conflict with the Master Agreement and this MOU. Official Time for local negotiations shall be granted in accordance with Article 2, Section 8.

14. The process of alerting NFFE bargaining unit employees of the expiration date of their PIV badges is an appropriate subject of bargaining at the local level.

15. The appropriate local Management official shall provide a copy of this MOU to the Local Union President upon receipt. This MOU will be posted on the VA website.

FOR THE AGENCY

Ainbint Munn
Labor Relations Specialist (LMR)
Department of Veterans Affairs

6/15/2016
Date

FOR THE UNION

Jeffrey Shapiro,
President
NFFE-IAM DVA Council

6/10/2016
Date

Attachment 1
Prior Process Flow

Below is a summary of the prior process flow for PIV credential and logical access issuance. It should take no more than five business days to complete.

1. Applicant completes necessary paperwork and forms for access, card issuance, and a background investigation.
2. Applicant is sponsored by an appropriate sponsor, such as the COR, HR liaison, or supervisor.
3. Applicant provides 2 forms of identification to the PIV issuance facility, and a Special Agreement Check (SAC), which includes electronic fingerprinting, is completed on the applicant.
4. Applicant completes required training, including security awareness training. The security awareness training is web-accessible, and applicants can self-register for this training. Some facilities run live training courses for security awareness training.
5. Applicant provides proof of required training to his or her sponsor.
6. An active directory account is established for the applicant.
7. Network access via a logon ID and password is requested and provided to the applicant.
8. Remote access and government-furnished equipment (GFE) is provided if necessary.
9. Applicants that will use GFE are provided RESCUE accounts and will access VA's IT network remotely using PIV credentials, once issued.
10. If the applicant is not going to be provided GFE, the only acceptable form of remote access is via the Citrix Access Gateway (CAG). Applicants using CAG on non-PIV-enabled devices, such as smartphones, will be directed to VA's Office of Information Security to secure a MobilePass soft token to access the network with multi-factor authentication. A MobilePass can only be issued to applicants that possess valid PIV credentials.
11. A background investigation is initiated, the applicant completes E-Quip forms, a background investigation is scheduled, and a transmittal notice sent to the sponsor.
12. Applicant receives PIV credential and establishes a PIN.

In a January 2014 memorandum, (attached) the Assistant Secretary for Operations, Security and Preparedness outlined the following temporary exceptions to PIV-only logical access, in the event a user experiences issues with card readers or cards:

“In the event that users encounter non-POA compliant systems, or have a PIV Card damaged, lost, stolen, or otherwise rendered inoperable . . . NSD will automatically revert users to POA status after 14 days unless the customer calls and asks for an extension. One extension will be granted for an additional 14 days, for a total of 28 days. Requests for future extensions must be considered on a case by case basis, and may be considered, routed, and granted through the customers' leadership chain. . . . Temporary Passwords will be activated . . . less than 10 minutes. . .”

Attachment 2
Improved Process Flow

Several improvements are planned for the PIV credential issuance process flow and enforcement, without impacting VA's mission:

1. Network accounts are created as soon as the applicant comes on board, on a contingency basis. Account information is withheld from the applicant pending SAC adjudication (normally within 3 days), required training, and if necessary, the background investigation has been initiated.
2. HR offices are encouraged to have new employees fingerprinted and the results of the FBI Criminal History and Name Check completed prior to EOD. If a background investigation is required, the investigation should be initiated into e-QIP pre EOD. Five (5) days after Entrance on Duty (EOD), and at least 3 days after fingerprints have been taken, applicant receives VA email address information and appears at the PIV issuance office to have a photograph taken and receive a PIV credential for physical and logical access.
3. If a PIV credential cannot be issued at this time for any reason, the applicant falls into a temporary exception category as outlined below.
4. Notification that a PIV credential is ready for pick-up, or that an applicant may now appear in person to be photographed will go to the supervisor, sponsor, or COR to communicate to the applicant, rather than directly to the applicant.
5. If the user is authorized to use CAG and cannot use a PIV for remote access, after receiving their PIV credential, the user will receive instructions, and based on the personal device to be used, either be provided a PIV reader or directed to secure a MobilePass soft token to access the network with multi-factor authentication.

Use-case exceptions and longer-term exemptions must be established in the event a PIV credential cannot be used for network logical access. The following exception and exemption cases are employed:

1. New Applicant Not Issued PIV in 5 Days – 14 day exception
2. Forgotten PIV or PIN – 1 day exception
3. Lost/Stolen/Defective PIV – 15 day exception
4. Equipment Malfunction Preventing PIV Use – 14 day exception
5. 508 Constraints – one year exemption via memorandum
6. Special Case Scenarios – exemptions issued via memorandum on a case-by-case basis lasting a maximum of one year

Research with NIST and other Federal agencies indicates that exceptions need to be renewable as often as is required to remediate the problem with PIV-only logical access. Therefore, the number of exceptions and exemptions granted to applicants will not be limited.

Attachment 3
Use Case Exceptions and Exemptions Process

New Applicant Process Flow:

1. Applicant completes necessary paperwork and forms for access, credential issuance, and a background investigation.
2. Applicant reports for biometrics capture, where a Special Agency Check (SAC) is done on the applicant, and provides two (2) forms of identification to the PIV issuance facility.
3. A NACI background investigation is initiated (not required for non-PIV credentials).
4. An active directory account is established for the applicant.
5. Applicant is sponsored for PIV credential by an appropriate sponsor, such as the COR, HR liaison, or supervisor.
6. Applicant completes required training, including security awareness training. The security awareness training is web-accessible, and applicants can self-register for this training. Some facilities run live training courses for security awareness training.
7. Applicant receives PIV credential and establishes a PIN.
8. Network access is provided to the applicant.
9. Remote access and government-furnished equipment (GFE) is provided if necessary.
10. Applicants who will use GFE are provided RESCUE accounts and will access VA's IT network remotely using PIV cards, once issued.
11. If the applicant is not going to be provided GFE, the only acceptable form of remote access is via the Citrix Access Gateway (CAG). Applicants will be instructed, based on the personal device to be used, and either provided a PIV reader, or directed to secure a MobilePass soft token to access the network with multi-factor authentication. A PIV credential is required to enroll in MobilePass.

New Applicant without PIV Issuance in First 5 Business Days:

1. Provided an applicant has completed steps 1-6 above, and still cannot get a PIV credential, the applicant contacts the National Service Desk at (855) 673-4357 and report the issue.
2. The National Service Desk, after verification of applicant identification, will put the applicant into the 14 day exception group and provide the applicant (now a system "user") with a logon ID and one-time password.
3. User logs onto the network with logon ID/password combination and changes one-time password.
4. Within 14 days, the user must report to PIV office to retrieve PIV credential.
5. Once the PIV credential is retrieved and activated, the PIV issuance office notifies the Helpdesk to put the user back in the enforcement group.

6. If the PIV credential is not provided by the PIV issuance office within 14 days, the user contacts the National Service Desk for another 14-day exception to technical enforcement, repeating this process from Step 1.

Lost, Damaged, Malfunctioning PIV Credential:

1. User contacts the National Service Desk at (855) 673-4357 and reports the problem with the credential.
2. The National Service Desk, after verification of user identification, puts the user into the 15 day exception group and provides the user with a logon ID and one-time password.
3. User logs onto the network with logon ID/password combination and changes one-time password.
4. User reports to local PIV badging office for replacement credential.
5. Once the PIV credential is retrieved and activated, the PIV issuance office notifies the Helpdesk to put the user back in the enforcement group.
6. If the replacement credential is not provided by the PIV issuance office within 15 days, the user contacts the National Service Desk for another 15-day exception to technical enforcement, repeating this process from Step 1.

Forgotten PIV Credential:

1. User contacts the National Service Desk at (855) 673-4357 and reports the forgotten PIV credential.
2. The National Service Desk, after verification of user identification, will put the user into the one day exception group and provide the user with a logon ID and one-time password valid for 24 hours.
3. User logs onto the network with logon ID/password combination and changes one-time password.

Forgotten PIV PIN:

1. User contacts the National Service Desk at (855) 673-4357 and reports the forgotten PIV PIN.
2. The National Service Desk, after verification of user identification, will put the user into the one day group and provide the user with a logon ID and one-time password valid for 24 hours.
3. User logs onto the network with logon ID/password combination and changes one-time password.
4. User reports to local PIV badging office to refresh the PIN.

Equipment Malfunction Preventing PIV Credential Logon:

1. User contacts the National Service Desk at (855) 673-4357 and report the problem.

2. The National Service Desk, after verification of user identification, will put the user into the one day group and provide the user with a logon ID and one-time password.
3. User logs onto the network with logon ID/password combination and changes one-time password.
4. The National Service Desk dispatches a technician to resolve the equipment situation or provide replacement equipment.
5. Once the technical resolves the situation or replaces the equipment, the technician closes the trouble ticket and has the user put back into the enforcement group.

Attachment 4
Frequently Asked Questions

As a new VA employee, how do I obtain a PIV card and VA network access?

1. Complete and submit the paperwork you received from your HR liaison (for government employees) or COR (for contract employees), as you need to be sponsored by a COR, HR liaison, or supervisor.
2. A network account and VA email address will be created for you, but you will not receive the information until your access is approved.
3. Make an appointment for your fingerprints to be taken. You can make an appointment at https://va-piv.com/. You will use the same link to make an appointment when your badge is ready. Remember, you'll need two forms of government ID (e.g. a driver's license, passport, or Social Security card) to get both your fingerprints and your PIV card. A list of acceptable documents is available on the appointment website.
4. You will need to have your fingerprints (Special Agreement Check/SAC) taken. Once submitted, the results are normally returned with 24-48 hours.
5. While your SAC is being completed, you can move forward with preparing for your access. You'll be required to complete security awareness training before you are given access to the VA network. The Information Security Awareness and Rules of Behavior training is available online at http://www.valu.va.gov/Home/Index, under "Mandatory Training." This training does not require VA network access or a VA email. Once you complete this training, provide your training certificate to your sponsor.
6. Next, you'll be initiated for a background investigation using OPM's e-QIP. This should take no more than five days. Please follow the instructions in that email to ensure you complete all necessary steps to ensure your background investigation is not delayed.
7. Once you complete your required segments of e-QIP, you certify and release it to the servicing human resources office. The servicing human resources office will review and release the case to OPM. Once OPM has the case and your investigation is scheduled along with the favorably adjudicated SAC, you will receive VA email address information and information to appear at the PIV issuance office to have a photograph taken and receive a PIV card for physical and logical access. For more information, access the VA PIV website https://va-piv.com/. You'll need to bring two forms of ID with you to the PIV issuance office.
8. After you get your PIV, you're ready to access the VA network!
9. You will receive government-furnished equipment (GFE) and a RESCUE account as necessary for remote access.
10. If you are required to use non-GFE or non-PIV enabled devices for VA network access, you will need a Citrix Access Gateway (CAG) account. For CAG access, after you receive a valid PIV, you will be directed to VA's Office of Information Security to secure a MobilePass soft token to access the network with multi-factor authentication.

How long will it take until I get my PIV card?
Your PIV card can be issued once your SAC has been favorably adjudicated and your background investigation has been scheduled by OPM. Your supervisor, sponsor, or COR will provide your VA email address information to provide to your local PIV office. Schedule an appointment to appear at the PIV issuance office to have a photograph taken and receive a PIV card for physical and logical access. (For more information, access the VA PIV website https://va-piv.com/). You'll need to bring two forms of ID with you to the PIV office.

What if I'm not in a VA facility? Can I still access the VA network?
You can! If you've been approved for remote access, you can use your PIV card to access VA's IT network remotely. If you're assigned GFE (aka, a VA laptop), and will need to access the VA network, you will receive a RESCUE account. If you don't have GFE, you will use your PIV to access the VA network through the Citrix Access Gateway (CAG). However, please note that both of these methods require your PIV. If you don't have your PIV, you'll need to retrieve it, or go to the nearest VA facility.

What if I can't use a PIV with my device? Can I still access the VA network?
If your device is not PIV-enabled (such as a smartphone), VA's Office of Information Security can help you secure a MobilePass soft token, which will allow you to use multi-factor authentication to access the VA network. You will need a valid PIV card in order to receive a MobilePass soft token.

Are there any exceptions or exemptions to the requirement to use a PIV card for logical access to the VA network?
Yes, there are. VA has approved the following exceptions and exemptions to the requirement:

1. New Applicant Not Issued PIV in 5 Days – 14 day exception
2. Forgotten PIV or PIN – 1 day exception
3. Lost/Stolen/Defective PIV – 15 day exception
4. Equipment Malfunction Preventing PIV Use – 14 day exception
5. 508 Constraints – one year exemption via memorandum
6. Special Case Scenarios – exemptions issued via memorandum on a case-by-case basis lasting a maximum of one year
7. Temporarily prevented by an application, equipment or use case listed in ForeFront Identity Manager (FIM)- until remediation of FIM exemption (National Service Desk tracks these exemptions)

Once granted, your exception or exemption can be renewed as often as is required to remediate the problem with PIV-only logical access.

I'm new. What should I do if my card hasn't been issued in the first five business days?

First, contact the National Service Desk (NSD) at (855) 673-4357 to report the issue. Once they verify your identity, the NSD will put you into the 14-day exception group and provide you with a logon ID and one-time password. You can use the logon ID/password combination to log onto the network. You will be prompted to change the one-time password during the logon process.

Within 14 days, you should report to PIV office to retrieve your PIV card. Once your PIV card is retrieved and activated, you must notify the NSD that you have your PIV card and no longer need the exception. If the PIV card is not provided by the PIV issuance office within 14 days, just contact the NSD for another 14-day exception to technical enforcement.

What should I do if an equipment malfunction is keeping me from logging on with my PIV Card?

First, contact the National Service Desk (NSD) at (855) 673-4357 to report the issue. If you're at a VA facility, the NSD can help you log on with an ID and password. Once they verify your identity, the NSD will put you into the 14-day exception group and provide you with a logon ID and one-time password. You can use the logon ID/password combination to log onto the network. You will be prompted to change the one-time password during the logon process.

The National Service Desk will dispatch a technician to resolve the equipment situation or provide replacement equipment. Once the technical resolves the situation or replaces the equipment, the technician closes the trouble ticket and you should return to logging on with your PIV card as usual.

What should I do if I forget my PIV Card or PIN?

If you forget your PIV **card** and are at a VA facility, contact the National Service Desk (NSD) at (855) 673-4357 to report the issue. Once they verify your identity, the NSD will put you into a 1-day exception group and provide you with a logon ID and one-time password valid for 24 hours. You can use the logon ID/password combination to log onto the network. You will be prompted to change the one-time password during the logon process. Your exception will expire after 24 hours, giving you time to retrieve your forgotten PIV card.

If you forget your PIV **PIN**, contact the National Service Desk (NSD) at (855) 673-4357 to report the issue. Once they verify your identity, the NSD will put you into the 1-day exception group and provide you with a logon ID and one-time password valid for 24 hours. You can use the logon ID/password combination to log onto the network. You will be prompted to change the one-time password during the logon process. Your exception will be valid for 24 hours, giving you time to report to the local PIV badging office to refresh the PIN.

What should I do if my PIV card is lost, damaged, or malfunctioning?
First, contact the National Service Desk (NSD) at (855) 673-4357 to report the issue. If you're at a VA facility, the NSD can help you log on with an ID and password. Once they verify your identity, the NSD will put you into the 15-day exception group and provide you with a logon ID and one-time password. You can use the logon ID/password combination to log onto the network. You will be prompted to change the one-time password during the logon process.

You should report to PIV office for a replacement card as soon as possible. Once your PIV card is retrieved and activated, the PIV issuance office will notify the NSD that you have your PIV card and no longer need the exception. If the PIV card is not provided by the PIV issuance office within 15 days, just contact the NSD for another 15-day exception to technical enforcement.