# Department of Veterans Affairs

# Memorandum

**Date:** JUL 28 2016

**From:** Assistant Secretary for Information and Technology (005)
Assistant Secretary for Operations, Security, and Preparedness (007)

**Subj:** PIV Logical Access Policy Clarification (VAIQ #7698332)

**To:** Under Secretaries, Assistant Secretaries, and Other Key Officials

1. The Office of Management and Budget requires each Federal agency to technologically enforce the use of Personal Identity Verification (PIV) credentials and Personal Identification Numbers (PIN) for logical access to all Federal IT systems and networks. All users requiring logical access to VA networks (which includes full-time and part-time employees, employees without compensation (WOC), contractors, volunteers, temporary employees, health professions trainees (HPTs), and affiliates, such as VSOs) must comply with this direction, with the exception of those identified in paragraph 2. Logical access is defined as access requiring validation of an individual's identity through some mechanism such as a PIN, card, biometric, or other token. It has the capability to assign different access privileges to different persons depending on their roles and responsibilities in an organization.

2. VA IT system users who will be employed for less than 179 days, or only undergo a Special Agreement Check (SAC) clearance per policy, will be required to obtain a "non-PIV" credential for logical access.

3. The VA Chief Information Officer (CIO), Chief Information Security Officer, and Deputy Secretary issued a series of memoranda requiring VA staff to use PIV credentials to access VA networks. On February 26, 2016, the VA CIO issued a memorandum (attached) directing OIT staff to issue network access to new employees and contractors only after they have a valid, operational PIV credential. The memorandum states that network access will not be granted to any contractor or employee who does not possess a current PIV credential fully enabled for logical access, with the exception of those identified in paragraph 4.

4. HPTs who enter the VA en masse in June and July will be issued usernames and passwords that are good for 14 days to give facilities time to process PIV applications.

5. The goal of this effort is to enforce PIV-only logical access to VA's network, and eventually to all IT systems, while reducing, and ultimately eliminating, the use of single factor authentication, i.e., logon ID and password combinations. It is imperative that this effort proceeds without inhibiting service to Veterans. Multiple technical, process, policy,

and personnel situations impact the Department's ability to immediately enforce full PIV-only logical access and completely eliminate the use of single factor authentication. These situations are being addressed, and VA is working toward full PIV-only logical access while ensuring that staffs maintain uninterrupted access to VA's network before, during, and after enforcement.

6. Attachment 1 summarizes the prior process flow for PIV credential issuance and logical access to VA's network. Attachment 2 outlines the improved PIV credential issuance and logical access process flow, and describes a set of temporary exceptions and longer-term exemptions for granting logical access only to PIV credential holders. Attachment 3 outlines specific steps applicants must follow to have exceptions and exemptions granted in the event PIV credential logical access is not possible. Attachment 4 addresses Frequently Asked Questions. The processes outlined in these attachments will be implemented immediately.

7. This memorandum supersedes the February 26. 2016. CIO memorandum titled, *Personal Identity Verification (PIV) Cards Issued Prior to Network Access,* (VAIQ #7645688).

8. If you have any questions regarding PIV credential issuance or the granting of logical access to VA's IT network, please have a member of your staff contact Charles R. Baumgardner, Executive Director of Enterprise Systems Engineering, at (202) 461-5152, or Charles.Baumgardner@va.gov or Thomas Napier, Director HSPD-12, at (202) 461-5082 or Thomas.Napier@va.gov.

LaVerne H. Council

Kevin T. Hanretta

Attachments (6):
Process Flow
Improved Process Flow
Use Case Exceptions and Exemptions Process
Frequently Asked Questions
Personal Identity Verification (PIV) Cards Issued Prior to Network Access
Restoration Guidance for Personal Identity Verification (PIV) Only Authentication

PIV Logical Access Policy Clarification

cc:
Deputy Assistant Secretary, Information Technology Resource Management (005F)
Acting Deputy Assistant Secretary, Office of Information Security (005R)
Deputy Chief Information Officer, Architecture, Strategy and Design (005E)
Deputy Assistant Secretary, Enterprise Program Management Office (005Q)
Deputy Assistant Secretary, Service Delivery and Engineering (005OP)
Deputy Chief Information Officer, Privacy and Risk (005PR)
Acting Deputy Director, Interagency Program Office (005J)
Deputy Chief Information Officer, Account Manager for Corporate (005C)

**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 Contracting Officers Representatives, 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-PIV Only Access (POA) compliant systems, or have a PIV Card damaged, lost, stolen, or otherwise rendered inoperable . . . National Service Desk (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 Entrance on Duty (EOD). If a background investigation is required, the investigation should be initiated into e-QIP, and when possible, completed by the applicant and scheduled at OPM pre EOD. Five (5) days after the new employee's (EOD), but at least 3 days after fingerprints have been taken, applicant receives his/her 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 obtain 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 National Institute for Science and Technology (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 pre-hire paperwork (I-9, OF-306, etc.) and forms for logical access/credential issuance.
2. Applicant completes a Special Agreement Check (SAC) as instructed by the local HR office or COR.
3. A Tier 1 NACI or higher level background investigation is initiated and reviewed by HR/Personnel Security Staff. (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 sponsoring office/official such as the supervisor, HR POC, or COR for contract staff.
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. The Applicant reports for biomedical capture and presents two (2) forms of identification to the PIV Registrar.
8. Applicant receives PIV credential and establishes a PIN.
9. Network access is provided to the applicant.
10. Remote access and government-furnished equipment (GFE) is provided if necessary.
11. Applicants who will use GFE are provided RESCUE accounts and will access VA's IT network remotely using PIV cards, once issued.
12. 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 NSD at (855) 673-4357 and report the issue.
2. The NSD 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 NSD for another 14-day exception to technical enforcement, repeating this process from Step 1.

**Lost, Damaged, Malfunctioning PIV Credential**:

1. User contacts the NSD at (855) 673-4357 and reports the problem with the credential.
2. The NSD 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 NSD for another 15-day exception to technical enforcement, repeating this process from Step 1.

**Forgotten PIV Credential:**

1. User contacts the NSD at (855) 673-4357 and reports the forgotten PIV credential.
2. The NSD 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 NSD at (855) 673-4357 and reports the forgotten PIV PIN.
2. The NSD 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 NSD at (855) 673-4357 and report the problem.
2. The NSD 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 NSD 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 supervisor and /or HR liaison (for government employees) or COR (for contract employees), as you need to be enrolled into the PIV system.
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. If you are being hired as a new federal employee at a VA Medical Center, your fingerprint appointment may already be scheduled for you as part of the pre-hire process. You should receive instructions from your local HR Office on how to complete this step. If you are not a new federal employee, or if you are instructed to do so, may use the PIV Appointment Scheduling website to make an appointment: https://va-piv.com.

   You will use the same link to make an appointment when your badge is ready. Remember, you will need two (2) 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 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. You will be instructed by your local HR Office or COR to complete a background investigation commensurate to your position in federal service. Please follow those instructions, to ensure you complete all necessary steps, including digital signature of your certification and release forms, so that your investigation is not delayed. Instructions to complete e-QIP may be sent you concurrently with step one of this process.
7. The servicing human resources office will review and release your investigation to Office of Personnel Management (OPM) for processing. Once your investigation is scheduled, along with a favorably adjudicated SAC, you will receive VA email address information and information to appear at the PIV issuance office to 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, and your network account has been established. Your sponsoring office will enroll you into the PIV system and provide instructions for you to contact 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 (i.e., 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 NSD 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, speak with your supervisor. Then if instructed to do so, contact the 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, speak with your supervisor. Then if instructed to do so, contact the 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 NSD 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 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 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, report the issue to your supervisor. Then contact the 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 the PIV office for a replacement card as instructed by your supervisor. 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.

# Department of Veterans Affairs

# Memorandum

**Date:** FEB 26 2016

**From:** Assistant Secretary for Information and Technology (005)

**Subj:** Personal Identity Verification (PIV) Cards Issued Prior to Network Access (VAIQ #7645688)

**To:** Under Secretaries, Assistant Secretaries, and Other Key Officials

1. Over the past several months, the Deputy Secretary and the Office of Information and Technology have issued several memoranda requiring the use of Personal Identity Verification (PIV) cards to log onto VA networks and information systems. This requirement is firmly rooted in both VA and Federal policy and regulations.

2. Using PIV cards to authenticate to our information systems is crucial because it provides Veterans more assurance that their sensitive data is protected as securely as possible. To ensure universal use of PIV cards for logical access, I am directing my organization to grant network and information system access to new employees and contractors *only after* they have a valid, operational PIV card. Network and information system access will not be granted to any contractor or employee who does not possess a current PIV card fully enabled for logical access.

3. If you have any further questions about PIV logical access or this direction, please have a member of your staff contact Susan Perez at susan.perez@va.gov or on 202.461.6552, or Gary Stevens at gary.stevens2@va.gov or on 202.632.7538.

LaVerne H. Council

cc:
Deputy Assistant Secretary, Information Technology Resource Management (005F)
Deputy Assistant Secretary, Office of Information Security (005R)
Deputy Chief Information Officer, Architecture, Strategy and Design (005E)
Deputy Chief Information Officer, Office of Product Development (005Q)
Acting Deputy Chief Information Officer, Service Delivery and Engineering (005OP)
Executive Director, Quality, Performance and Oversight (005X)
DCIO, Account Manager for Corporate (005C)
Acting Deputy Director, Interagency Program Office (005J)

**Department of Veterans Affairs**

# Memorandum

Date: AUG 3 1 2015

From: Assistant Secretary for Information and Technology, Chief Information Officer (005)

Subj: Mandatory Use of PIV Card Authentication for VA Information System Access (VAIQ #7633050)

To: Under Secretaries, Assistant Secretaries, and Other Key Officials

1. VA has made significant progress in improving its use of Personal Identity Verification (PIV) cards for logical access to the VA network, but we must make this a matter of business practice and management policy. Currently, only 50 percent of those VA employees, not involved in direct patient care, are logging on the VA network each day with a PIV card. I am asking for your personal commitment that all employees, contractors, and other system users within your respective organizations, required to use PIV authentication, begin using their PIV card immediately. Only by such commitment and diligence will VA will improve its overall PIV card usage and compliance with existing Presidential Directives. Full implementation of PIV card usage to access information systems takes VA forward in cybersecurity and the protection of Veteran information.

2. Secondly, I am asking for your assistance in implementing technical enforcement of PIV card usage to gain access to VA systems. OI&T recently resumed technical enforcement of PIV cards to access VA information systems in response to elevated VA cybersecurity concerns and Federal CIO priorities. We are currently focused on OI&T systems administrators and those with elevated privileges. However, we must broaden our efforts to include VA users without elevated privileges. My staff will be reaching out to your respective staffs to form a cross-functional team to plan and implement technical enforcement of PIV card usage across VA.

3. On June 11, 2015, Tony Scott, the Federal CIO, identified a series of "Priority Cybersecurity Action Items" to be accomplished over a 30-day period to rapidly improve the Federal cyber security posture. One of the major action items was for each agency to achieve 100% compliance with PIV card logical access by July 15, 2015. Toward that end, VA's Chief Information Security Officer issued two memoranda on June 30, 2015, *Mandatory Use of PIV Multifactor Authentication to VA Information Systems* and *Mandatory Use of PIV Multifactor Authentication for Users with Elevated Privileges*, requiring all VA system users, both with normal access privileges and with elevated privileges, to immediately being logging onto VA networks with a PIV card. The only exception to this requirement is for VHA staff involved in direct patient care, currently designated as physicians and nurses. On July 9, 2015, the Deputy Secretary further reiterated the PIV card requirement, *Implementation of Federal Identity Verification (PIV) Credentials for Federal Employee*

*and Contractor Access to VA IT Systems*, directing the Department's senior leaders to remove any barriers to PIV card use in VA. The memoranda discussed above are attached.

4. The requirement for PIV card log-on is not new. Homeland Security Presidential Directive 12 (HSPD-12), signed in 2004, and Federal Information Processing Standard (FIPS) 201, published in 2005, outline the requirement and technical specifications for the use of PIV cards for physical and logical access to Federal facilities and information systems. As a result, VA policy codified in VA Handbook 6500 requires all VA IT systems to be PIV-enabled and requires the use of multifactor authentication when using a local, network, or remote account to log into a VA information system.

5. Thank you in advance for your support and partnership on PIV implementation to improve assurance of VA operations and daily services for the Veteran. Please confirm your lead representatives for the PIV technical team to Rusty Baumgardner at (202) 461-5152 or email at charles.baumgardner@va.gov. Users who need help using their PIV card or have a damaged or missing PIV card are to contact the National Service Desk at (855) 673-4357 for assistance. For PIV policy questions, please contact Mr. John Oswalt, Associate Deputy Assistant Secretary for Policy, Privacy, and Incident Response at (202) 632-7489 or email at john.oswalt@va.gov.

LaVerne H. Council

Attachments

cc:
Deputy Assistant Secretary, Information Technology Resource Management (005F)
Deputy Assistant Secretary, Information Security (005R)
Deputy Chief Information Officer, Architecture, Strategy and Design (005E)
Deputy Chief Information Officer, Product Development (005Q)
Deputy Chief Information Officer, Service Delivery and Engineering (005OP)
Executive Director, Quality, Performance and Oversight (005X)
Deputy Director, Interagency Program Office (005J)
Deputy Chief Information Officer, Advocate for Corporate (005C)

**Department of Veterans Affairs**

# Memorandum

**Date:** JUL 9 - 2015

**From:** Deputy Secretary (001)

**Subj:** Implementation of Federal Personal Identity Verification (PIV) Credentials for Federal Employee and Contractor Access to VA IT Systems (VAIQ# 7614373)

**To:** Under Secretaries, Assistant Secretaries, and Other Key Officials

1. Office of Management and Budget (OMB) memorandum M-11-11 requires the continued implementation of Homeland Security Presidential Directive 12 (HSPD-12) - *Policy for a Common Identification Standard for Federal Employees and Contractors.* HSPD-12 is a strategic initiative intended to enhance security, increase Government efficiency, reduce identity fraud, and protect personal privacy. HSPD-12 requires agencies to follow specific technical standards and business processes for the issuance and routine use of Federal Personal Identity Verification (PIV) smartcard credentials.

2. Chief Information Security Officer Stanley Lowe issued two memoranda on June 30, 2015, reiterating the requirement to use PIV credentials to access VA's information systems. The first memorandum, *Mandatory Use of PIV Multifactor Authentication to VA Information Systems*, requires that by July 15, 2015, all VA information system users not responsible for direct patient care must use PIV credentials to gain access to any VA information system. The second memorandum, *Mandatory Use of PIV Multifactor Authentication for Users with Elevated Privileges,* requires immediate use of PIV credentials for VA information system users with elevated privileges.

3. VA is committed to complying with these requirements and implementing the use of PIV credentials in accordance with Federal Information Processing Standard 201. Our commitment to our Veterans to securely deliver benefits and services requires an expedited and comprehensive implementation approach. Under Secretaries, Assistant Secretaries, and Key Officials with personnel involved in the implementation of these requirements must fully cooperate with the HSPD-12 Working Group by providing the necessary resources and staffing, when requested. Moreover, I expect that Departmental senior leaders will mitigate any obstacles preventing the implementation of these requirements as quickly as possible to resolve the impasse that is precluding implementation of the required capability. I plan on using the CRISP Working Group and OMR's as forums to resolve any issues that require my intervention.

**Department of Veterans Affairs**

# Memorandum

Date: June 30, 2015

From: Deputy Assistant Secretary for Information Security (005R)

Subj: Mandatory Use of PIV Multifactor Authentication to VA Information System (VAIQ# 7613595)

To: See Addressees Below

1. By the authority granted my position under the Federal Information Security Modernization Act of 2014 (44 U.S.C. 3554), I am directing that the actions stated in this memorandum be fully and completely implemented to comply with VA, Office of Management and Budget (OMB), and Department of Homeland Security requirements regarding multifactor authentication to VA's information systems.

2. Homeland Security Presidential Directive 12 (HSPD-12), signed in 2004, and Federal Information Processing Standard (FIPS) 201, published in 2005, outlined the requirement and technical specifications for the use of Personal Identity Verification (PIV) cards for physical and logical access to Federal Facilities and information systems. VA Handbook 6500 requires all VA IT systems to be PIV-enabled and requires the use of multifactor authentication when using a local, network, or remote account to log into a VA information system. As directed by then Secretary Shinseki, in his memorandum dated April 29, 2011, use of PIV credentials as the common means of identification and authentication for physical and logical access to VA facilities, networks and Information systems is required.

3. Therefore, effective July 15, 2015, all VA information system users not responsible for direct patient care must use their PIV card and PIN to gain access to any VA information system. Users who need help using their PIV card should contact the National Service Desk at (855) 673-4357.

4. If there are any questions about this requirement, please contact Gary Stevens at Gary.Stevens2@va.gov or (202) 632-7538.

Stanley F. Lowe

**Department of Veterans Affairs**

# Memorandum

Date: June 30, 2015

From: Deputy Assistant Secretary for Information Security (005R)

Subj: Mandatory Use of PIV Multifactor Authentication for Users with Elevated Privileges (VAIQ# 7613597)

To: See Addressees Below

1. By the authority granted my position under the Federal Information Security Modernization Act of 2014 (44 U.S.C. 3554), I am directing that the actions stated in this memorandum be fully and completely implemented to comply with VA, Office of Management and Budget (OMB), and Department of Homeland Security requirements regarding multifactor authentication to VA's information systems.

2. Homeland Security Presidential Directive 12 (HSPD-12), signed in 2004, and Federal Information Processing Standard (FIPS) 201, published in 2005, outlined the requirement and technical specifications for the use of Personal Identity Verification (PIV) cards for physical and logical access to Federal Facilities and information systems. VA Handbook 6500 requires all VA IT systems to be PIV-enabled and requires the use of multifactor authentication when using a local, network, or remote account to log into a VA information system. As directed by then Secretary Shinseki, in his memorandum dated April 29, 2011, use of PIV credentials as the common means of identification and authentication for physical and logical access to VA facilities, networks and Information systems is required.

3. Therefore, effective immediately, any VA information system user with <u>any type of elevated privileges</u> must use their PIV card and PIN to gain access to any VA information system. Users with elevated privileges are someone other than a general user or user who conducts routine activities. Privileged users are authorized (and therefore, trusted) to perform administrative functions and execute commands that ordinary users are not authorized to perform on an information system involving the control, monitoring, or administration of the system. Users who need help using their PIV card should contact the National Service Desk at (855) 673-4357.

**Department of Veterans Affairs**

# Memorandum

**Date:** November 12, 2014

**From:** Deputy Assistant Secretary for Information Security, Office of Information and Technology (005R)

**Subj:** Two-Factor Authentication for Remote Access to the VA Network (VAIQ# 7544141)

**To:** See Addressee List

1. Consistent with my role as the VA Chief Information Security Officer (CISO), it is my expectation that all remote access users, to include VA employees, contractors, and other third parties that possess personal identity verification (PIV) enabled, Windows-based government furnished equipment (GFE), must use a PIV card to authenticate to the network through the Remote Enterprise Security Compliance Update Environment (RESCUE). This is in response to FISMA and FISCAM findings whereby VA is not compliant with OMB guidance and needs to implement a two-factor authentication solution for remote access throughout the VA. I am directing the VA Network and Security Operations Center (NSOC) to implement this requirement by January 20, 2015.

2. Analysis of current PIV card usage indicates minimal, if any, negative impact to users when they authenticate to the VA network exclusively using their PIV card. However, to help ensure personnel are able to access applications or programs remotely, please identify any unique capabilities or applications that may be negatively impacted when a PIV card is required to authenticate to the network remotely. Please provide all input, including an explanation of the impact, to the Office of Cyber Security (OCS) via VAIQ by close of business November 21, 2014 so that remediation can be resolved prior to the January 20, 2015 enforcement date.

3. This requirement will not affect personnel with non-Windows based GFE devices, such as Apple devices or those personnel who use Citrix Access Gateway (CAG) to access the VA network. They can continue to use CAG while an alternate two-factor authentication solution is developed.

4. This requirement does not currently apply to mobile devices.

5. Failure to comply with this requirement will negatively impact the security posture of the VA and impedes VA's efforts to comply with Federal directives on the use of PIV cards for remote access to VA's networks and information technology resources. If there are questions, please contact Gary Stevens, Director, Office of Cybersecurity, at Gary.Stevens2@va.gov or 202-632-7538.

Stanley F. Lowe

Addressees:
Executive in Charge and Chief Information Officer (005)
Deputy Assistant Secretary, Information Technology Resource Management (005F)
Deputy Chief Information Officer, Architecture, Strategy and Design (005E)
Deputy Chief Information Officer, Service Delivery and Engineering (005OP)
Deputy Chief Information Officer, Product Development (005Q)
Executive Director, Quality, Performance and Oversight (005X)
Deputy Director, Interagency Program Office (005J)
Deputy Chief Information Officer, Advocate for Corporate (005C)

# Memorandum

## Department of Veterans Affairs

**Date:** JAN 1 6 2014

**From:** Assistant Secretary for Operations, Security, and Preparedness (007)

**Subj:** Restoration Guidance for Personal Identity Verification (PIV) Only Authentication (POA) (VAIQ #7324110)

**To:** Under Secretaries, Assistant Secretaries and Other Key Officials

1. Rollout of the Personal Identity Verification (PIV) Only Authentication (POA) commenced in the fourth quarter of fiscal year 2013. This user account based enforcement of PIV smartcard authentication will be deployed nationally to all Department of Veterans Affairs (VA) users regardless of location or office, unless the Secretary of Veterans Affairs determines that implementation is likely to have an adverse impact to Veterans Care and Health Services.

2. Upon implementation, Information Technology system users will be required to insert their PIV Card into their system's PIV Card reader, and enter their PIV Personal Identification Number (PIN), each time they log in or unlock a desktop computer, laptop computer, or other device which accesses government information systems. Minimum exceptions to this POA process will be approved and that list will be monitored by the appropriate PIV Only Authentication Integrated Project Team Lead for that Administration or Staff Office (attached).

3. In the event that users encounter non-POA compliant systems, or have a PIV Card damaged, lost, stolen, or otherwise rendered inoperable, guidance is defined in paragraph 4 concerning the time period for which a user may be reverted from PIV smartcard to password authentication.

4. National Service Desk (NSD) will use Service Level Requirement (SLR) 2.4 standards to respond to users experiencing issues with PIV smartcard authentication.

   a. NSD will meet SLR 2.4 at the target level. These metrics apply VA-wide, to all Staff Offices and Administrations.

   b. 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.

Interim Restoration Guidance for Personal Identity Verification (PIV) Only Authentication (POA) (VAIQ #7324110)

c. Temporary Passwords will be activated: under or less than 10 minutes on tier 1 tickets.

d. NSD maintains a Swift Action and Triage Initiation (SWAT) process. In the event of catastrophic failure of one or more PIV systems the NSD will stand-up a SWAT team to utilize all personnel with proper permissions to generate temporary and emergency passwords for all impacted customers.

5. Local facilities have the following responsibilities:

a. Emergency password generation will be coordinated at the local level with the respective Office of Information Technology (OIT) System Administrator to facilitate the timely resolution of emergencies. In cases where a password is locally created, the password will expire after 1 day.

b. The Administrations (VHA, VBA, and NCA) will oversee this process to ensure security and issuance of emergency passwords. An After Action Report outlining the justification for the emergency local approval will be required within 1 day of password creation.

6. Please note that this guidance does not apply to exemptions granted due to a system incompatibility with PIV Cards (e.g. MRI Scanner incompatible with the PIV System).

7. This policy is valid until superseded or revised by Homeland Security Presidential Directive-12 Program Management Office.

8. If you have questions, feel free to contact Tom Napier, Director, HSPD-12 PMO at (202) 461-5082.

Kevin T. Hanretta

Kevin T. Hanretta

Attachment

Distribution:

PIV Only Authentication Integrated Project Team Leads (POA IPT) (Attached)

**PIV Only Authentication Integrated Project Team Leads (POA IPT)**

**PLEASE ENSURE DISTRIBUTION TO THE PERSONNEL BELOW IN YOUR ORGANIZATION:**

**VHA** – Bob Phillips
**VBA** – Debra Young, William Hutson
**NCA** – Art Smith
**OSP** – Joshua Blockburger
HSPD-12 – Thomas Napier, Hector Marcayda, Matthew Robinson, John Horton
**OIT** – Rodney Hampton
SDE – Tracy Perkins, Giselle Hernandez-Bethea, Eric Jurasas,
Meah Shahabuddin,
NSD – Wendy Owens, John Frazier