DEPARTMENT OF VETERANS AFFAIRS
Veterans Benefits Administration
Washington, D.C. 20420

September 22, 2016

VBA Letter 20-16-08

Director (00)
All VBA Regional Offices and Centers

SUBJ: Internal VBA Systems Access for Claimant and Appellant Representatives

Purpose

The purpose of this letter is to provide procedures to grant access to VA information systems to accredited claimant and appellant representatives. Users cannot access internal systems without a Personal Identity Verification (PIV) badge; therefore, in order for accredited claims agents, attorneys, and employees of Veterans Service Organizations (VSOs) to gain access to VBA systems, VA must issue them a PIV badge.

VA has a responsibility to preserve the ability of a claimant's representative to access that claimant's VA claims records while complying with Homeland Safety Presidential Directive 12 (HSPD 12), Federal Information Processing Standards Publication (FIPS PUB 201-2), and applicable laws, rules, and regulations related to access to secure government information systems.

To achieve this balance, VBA follows the policies and procedures of the VA Office of Information Security, specifically in regards to completing identity verification, background investigations, and PIV badge issuance to any individual granted access to VA information systems.

Prerequisites for System Access

Due to the cost involved in establishing system access, VA will only establish access for individuals:

- Accredited by VA's Office of General Counsel (OGC) to represent Veterans as a claims agent, attorney, or employee of a Veterans Service Organization and
- Designated by one or more Veterans to represent him or her in pursuing a claim or appeal for VA benefits.

If a person requesting access does not meet these requirements, VA will not issue a PIV card and establish system access until the need for such access is demonstrated.

VBA System Access Security Requirements

The security requirements for VBA systems access are:

- Fingerprinting (favorable outcome);
- Office of Personnel Management (OPM) background investigation (initiated);
- Completed information security training;
- Completed Optional Form (OF) - 306, Declaration of Federal Employment, and
- Signed Rules of Behavior (ROB).

Upon successful adjudication of the background investigation and issuance of a PIV badge, VA will grant access to the VA network and to the Veterans Benefits Management System (VBMS). An individual granted access to VBMS will have a user role of "POA" and will be associated with the electronic records of Veterans he or she represents.

The VA National Service Desk (NSD) will provide IT support to representatives with remote access to VA systems. The National Service Desk is available to provide assistance 24 hours a day, 7 days a week at 1-855-NSD-HELP or 1-855-673-4357.

Processing VA System Access Requests

To request remote access, accredited representatives should submit a completed OF-306, *Declaration of Federal Employment* and VA Form 20-0344, *Annual Certification of Veterans Status and Veteran-Relatives* to the Change Management Agent (CMA) at the closest regional office. A list of CMAs is available online at:

http://www.benefits.va.gov/COMPENSATION/cma-poc.asp

Upon receipt of a request, the CMA will send the accredited representative an e-mail acknowledging receipt of his or her documents, providing the requestor with the CMA's contact information, and informing the requestor a background investigation will be initiated.

The Information Security Officer (ISO) will verify accreditation or employment with a VSO by searching the Office of General Counsel's (OGC) online Accreditation Database. If the requestor is not accredited, the ISO will refer the case to the VBA's Office of Field Operations (OFO) via email at ofo.vbaco@va.gov. OFO will review the circumstances of the application, communicate with OGC, and if not able to resolve the issue, refer the requestor to OGC to pursue accreditation.

Under exceptional circumstances, OGC may direct VBA to issue a PIV card and grant systems access to an individual who is not an accredited representative. When these situations occur, OFO will contact the regional office directly to provide further instructions.

Regional Office Change Management Agent

The CMA will be the representative's primary point of contact throughout the process. The CMA's role is to ensure timely action is being taken on the representative's request for access and to respond to status inquiries from representatives seeking access. The CMA will also accept documents and forward them to the appropriate office or individual within the RO.

Note: Under no circumstances is the CMA permitted to keep or otherwise maintain application documents containing representative's personally-identifiable information once it has been sent to the appropriate office or individual for action.

Regional Office Human Resource Liaison / Specialist

The Human Resource (HR) Liaison / Specialist is responsible for coordinating PIV card issuance, receiving the completed OF-306 and VA Form 20-0344, and providing security requirements to the requestor. If the attorney fails the background investigation based on HSPD-12 denial guidelines, the HR Liaison / Specialist will deny access and inform both OGC and OFO immediately. HR and Human Resources Centers will follow the same background investigation guidelines used for VSO employees.

Regional Office Training Manager

The RO Training Manager is responsible for establishing a Talent Management System (TMS) account so the requestor can complete required information security training and digitally sign the ROB. Upon the requestor's successful completion of information security training and receipt of a signed ROB document, the regional office may grant access to VBA systems.

Power of Attorney (POA) Code for Accredited Representatives

To gain access to Veteran records, a representative must have a personal login to the VA network and appropriate VA systems **and** be associated with a POA code. For example, an attorney named John Q. Public would receive a login under his name and a POA code in his name as well. In order for this attorney to access client records, a Veteran must have "John Q Public" selected as his or her POA code in the system.

Agents or attorneys can also be associated with multiple POA codes. An example of this would be attorney John Q. Public representing Veterans personally and also on behalf of an organization such as Disabled American Veterans. In this scenario, John Q. Public's account would be associated with both the John Q Public and Disabled American Veterans POA codes.

Note: Association in the OGC accreditation database or a written statement from an additional organization is required prior to associating an account with multiple POA codes.

Some accredited representatives do not have a POA code in the system. For these representatives, the regional office may still guide the representative through the PIV process and establish remote network access, but **may not** grant access to VBMS or any other VA system. When such a representative is found, the regional office will contact the NSD and open a ticket for POA code establishment. NSD personnel will assign this task to the appropriate office within VBA Central Office and notify the regional office of completion.

Questions

Questions regarding accreditation may be directed to the VA Office of General Counsel via e-mail to ogcaccreditationmailbox@va.gov.

Questions regarding other matters may be sent to the Office of Field Operations via e-mail to ofo.vbaco@va.gov.

/s/
Thomas J. Murphy
Principal Deputy Under Secretary for Benefits
Performing the Duties of
Under Secretary for Benefits

Enclosure: Attachment A: Access Process

Attachment A: Access Process

Step 1: To request VA system access, a representative must provide:
OF-306, Declaration of Federal Employment – (a) Complete OF-306, Declaration of Federal Employment (b) CMA sends representative acknowledgement e-mail (c) CMA submits to local Human Resource Liaison/Specialist
Veteran Status and Relative Status – (a) Complete VA Form 20-0344, Annual Certification of Veteran Status and Veteran-Relatives (b) CMA submits to local Human Resource Liaison/Specialist
Step 2: The CMA:
Request a background Investigation from their local Human Recourse Liaison/Specialist – (a) The local Human Resource Liaison/Specialist initiates background investigation and provides the CMA with an e-QIP link. The CMA provides the link information to the representative. (b) Complete required background investigation including the Special Agreement Check (SAC) for fingerprinting. The SAC is normally completed within 1-3 days of fingerprint submission (c) If the representative does not pass the background investigation or if the fingerprints are not acceptable, the CMA will notify OFO.
Initiates training requirements - (a) CMA contacts local Training Manager for creation of the Talent Management System (TMS) account (b) Training Manager creates TMS account and assigns HIPPA and TMS VA 10176 to representative (c) The CMA provides the TMS account information to the representative to complete the required training
Requests VA Network Access and User Account – (a) CMA submits VA Form 20-8824e, *Common Security Services (CSS) User Access Request* to ISO via CSEM

(b) CMA submits VA Form 20-8824f , *Veteran Benefits Administration/Central Office Network Access Request* to their local ISO

(c) ISO reviews and approves 20-8824f and submits to local IT staff for implementation and to create user account

(d) The IT staff sends account creation email and instructions to obtain network access credentials to the CMA

Step 2: After completion of these requirements, the CMA will

Request PIV –

(a) The Human Resource Liaison / Specialist serves as the representative's PIV Sponsor. He or she initiates the PIV card request in PIV enrollment portal.

(b) The CMA will advise the representative of the need to have two forms of ID (acceptable forms of ID listed on FIPS 201-2, section 2.7, and Identity Document Matrix)

(c) The CMA will assist the representative with scheduling an appointment with a badge office

i. See the list of PCI Facilities to find the closest one

ii. You must bring two forms of ID with you to your appointment

iii. Use the new VA PIV Scheduling tool. Click here to determine if your local PCI Facility is utilizing the tool

(d) Activate PIV card.

Provide the representative with VA System Access –

CMA to provide login instructions to representative