

representative to obtain permission to do so. The COTP or an on-scene representative may be contacted via VHF Channel 16. Vessel operators given permission to enter or operate in the safety zone must comply with all directions given to them by the COTP or an on-scene representative.

Dated: June 16, 2022.

**D.P. Montoro,**

*Captain, U.S. Coast Guard, Captain of the Port Lake Michigan.*

[FR Doc. 2022-13310 Filed 6-23-22; 8:45 am]

**BILLING CODE 9110-04-P**

## DEPARTMENT OF HOMELAND SECURITY

### Coast Guard

#### 33 CFR Part 165

[Docket No. USCG-2022-0523]

#### Safety Zone; Seafair Air Show Performance, 2022, Seattle, WA

**AGENCY:** Coast Guard, DHS.

**ACTION:** Notification of enforcement of regulation.

**SUMMARY:** The Coast Guard will enforce the annual Seafair Air Show Performance safety zone on Lake Washington, Seattle, WA, from 10 a.m. until 4 p.m. on August 4th and from 8 a.m. until 5 p.m. on August 5th, 6th, and 7th 2022. This action is necessary to ensure the safety of the public from inherent dangers associated with these annual aerial displays. During the enforcement period, no person or vessel may enter or transit this safety zone unless authorized by the Captain of the Port or his designated representative.

**DATES:** The regulations in 33 CFR 165.1319 will be enforced from 10 a.m. until 4 p.m. on August 4th and from 8 a.m. until 5 p.m. on August 5th, 6th, and 7th 2022.

**FOR FURTHER INFORMATION CONTACT:** If you have questions about this notice of enforcement, call or email Lieutenant Peter J. McAndrew, Sector Puget Sound Waterways Management Division, Coast Guard; telephone (206) 217-6051, email [SectorPugetSoundWWM@uscg.mil](mailto:SectorPugetSoundWWM@uscg.mil).

**SUPPLEMENTARY INFORMATION:** The Coast Guard will enforce the Seafair Air Show Performance safety zone in 33 CFR 165.1319 from 10 a.m. until 4 p.m. on August 4th and from 8 a.m. until 5 p.m. on August 5th, 6th, and 7th 2022 unless canceled sooner by the Captain of the Port. The specific boundaries of the safety zone are listed in 33 CFR 165.1319(b).

In accordance with the general regulations in 33 CFR part 165, subpart C, no person or vessel may enter or remain in the zone except for support vessels and support personnel, vessels registered with the event organizer, or other vessels authorized by the Captain of the Port or designated representatives. Vessels and persons granted authorization to enter the safety zone must obey all lawful orders or directions made by the Captain of the Port or his designated representative.

The Captain of the Port may be assisted by other federal, state and local law enforcement agencies in enforcing this regulation.

In addition to this notice of enforcement in the **Federal Register**, the Coast Guard will provide the maritime community with advanced notification of the safety zone via the Local Notice to Mariners and marine information broadcasts on the day of the event.

If the COTP determines that the safety zone need not be enforced for the full duration stated in this notice of enforcement, he may use a Broadcast Notice to Mariners to grant general permission to enter the regulated area.

Dated: June 17, 2022.

**P.M. Hilbert,**

*Captain, U.S. Coast Guard, Captain of the Port Puget Sound.*

[FR Doc. 2022-13506 Filed 6-23-22; 8:45 am]

**BILLING CODE 9110-04-P**

## DEPARTMENT OF VETERANS AFFAIRS

### 38 CFR Parts 1 and 14

RIN 2900-AQ81

#### Individuals Using the Department of Veterans Affairs' Information Technology Systems To Access Records Relevant to a Benefit Claim

**AGENCY:** Department of Veterans Affairs.

**ACTION:** Final rule.

**SUMMARY:** The Department of Veterans Affairs (VA) issues this final rule amending its regulations addressing when VA will allow individuals and VA recognized service organizations who are assisting claimants in the preparation, presentation, and prosecution of their benefit claims before VA to access specific VA's information technology (IT) systems to review VA records relevant to their clients' claims. This final rule addresses who is permitted, and under what circumstances, to directly access VA records and other claims-related information through specific VA IT

systems during representation of a claimant in a claim for VA benefits. This rule also outlines the appropriate behavior while using VA's IT systems to access records and the consequences for individuals who mishandle such access. This rulemaking, however, does not address general issues involving management of access to VA physical facilities or VA's disclosure of claimants' private information through any means other than direct access to the specific VA IT systems.

**DATES:** This final rule is effective July 25, 2022.

**FOR FURTHER INFORMATION CONTACT:**

Carling K. Bennett, Management and Program Analyst, Office of Administrative Review, Department of Veterans Affairs, 810 Vermont Avenue NW, Washington, DC 20420, 202-632-5347 (this is not a toll-free number).

**SUPPLEMENTARY INFORMATION:** On February 19, 2020, VA published a proposed rule in the **Federal Register** at 85 FR 9435-41, to clarify when an individual providing representation on a claim may access a claimant's automated records now that VA has transitioned to primarily processing VA benefit claims electronically. VA provided a 60-day public comment period and invited interested persons to submit written comments on or before April 20, 2020. In response to the proposed rule, VA received 15 written comments. The commenters included VA-accredited attorneys, law firms, VA-recognized veterans service organizations (VSOs), non-profit corporations, a legal clinic, a law student, and a trade association. In preparing this final rule, VA carefully considered all comments received in response to the proposed rule and addresses them below according to topic. In this final rule, VA focuses its discussion on changes from the proposed revisions based on comments received during the comment period and VA's further consideration of the issues raised by the comments. By clarifying through this rulemaking: (1) who is eligible to apply for remote access to VA IT systems for the purpose of representing, or assisting in the representation of, claimants on their VA benefits claims, and (2) the basic parameters on the privileges that will be granted to the approved VA IT system users, VA will provide transparency to Veterans and beneficiaries as to who may receive information from VA by accessing specific VA IT systems remotely. However, this rule does not change the ability of VA to disclose a claimant's private claim information through other methods to the claimant's

appointed attorney or agent of record or to the representatives of the claimant's appointed VSO of record as those who do not seek optional system access under the amended regulations may continue to receive records from VA as provided under the other provisions in 38 CFR part 1. Likewise, the rule does not change the ability of VA to disclose a claimant's private claim information through other methods to certain other individuals under an authorization that is not reliant on representation. *See* 38 CFR 1.500–1.527 (generally addressing the release of information from VA claimant records).

#### **A. Comments Concerning Competent Representation and Meaningful Access to Records, Including Comments Concerning the Proposed Removal of the Note to 38 CFR 14.629**

This rulemaking was necessary because, as several of the commenters pointed out, the regulations, policies, and procedures governing attorneys, agents, and VSO representatives and their staffs' access to the VA IT systems have been applied inconsistently in the past, and it is important that Veterans are aware of who may be able to access their claims information maintained in VA IT systems. VA believes that some of the variation of the application of these regulations, policies, and procedures may be due to the note that follows current 38 CFR 14.629(c), which indicates that systems access to claims records may be provided to legal interns, law students, paralegals, and VSO support staff, who are working under the supervision of an accredited individual designated under § 14.631(a) to represent the claimant. VA is aware that some paralegals, interns, and support staff have been approved for access to Veterans Benefits Management System (VBMS) in the past even though VBMS is not one of the VA IT systems listed in 38 CFR 1.600. VA is also aware that some VA-accredited IT system users and their staffs have been granted broad privileges within VBMS allowing certain users to view records of claimants for whom they do not hold the power of attorney (POA) so long as they are affiliated with the individual attorney or VSO that has been designated as the POA pursuant to 38 CFR 14.631.

VA proposed amending 38 CFR 1.600 through 1.603 to establish that only an individual who is accredited by VA pursuant to 38 CFR 14.629 as an attorney, agent, or representative of a VA-recognized service organization may be granted direct access privileges to VA IT systems, and within those systems, would only be permitted to access the

records of claimants for whom that individual holds POA pursuant to 38 CFR 14.631. VA received twelve comments expressing general opposition to such restrictions on access. Most of these commenters urged VA to promulgate a broader rule allowing systems access to individuals who assist in the representation of a claimant before VA, including accredited associate attorneys and agents, paralegals, law students, interns, and other non-lawyer support staff. The commenters also urged VA to allow for more expansive permissions within the systems, to include the ability to view records of claimants for whom the users do not hold the POA as long as the users are affiliated with the individual or organization who does hold the POA. Commenters stated that VA's decision to preclude direct system access to electronic records to individuals who assist in the representation of a claimant before VA would undermine the ability of the appointed attorney and agent to provide competent representation and deprive their clients of critical information. One commenter supported the overall changes and agreed with the spirit of VA's proposed amendments, applauding VA's efforts to ensure that Veterans' data is protected.

VA's objective with this rulemaking continues to be to provide the individual or VSO that is appointed to provide representation on the claim suitable remote access so that individual or VSO may provide responsible, qualified representation consistent with VA's policies. However, the comments have made clear that the office structure of the VA-accredited attorneys and agents has evolved to more of a team environment, and now, attorneys and agents have a strong preference that affiliated attorneys and agents as well as support staff should be able to assist in accessing VA documents on behalf of the claimants that the accredited attorney or agent is representing. VA recognizes that limiting systems access to the sole practitioner designated as the representative of record on the VA Form 21–22a, *Appointment of Individual as Claimant's Representative*, may hamper VA's goals to streamline the appeals process and to transition from a cumbersome, paper-intensive process to an efficient electronic environment in order to provide a faster, more accurate and transparent claims process. In response to these comments and upon further consideration, VA revises the framework of the proposed rule by broadening access to claimants' electronic records to certain individuals assisting in the representation of a

claimant before VA. VA believes that the security risk posed to the VA IT systems and the information within them can be largely managed through internal policies and added safeguards. Such safeguards include regular, recurring reviews of who has access and under what circumstances, plus recurring certifications of training and acknowledgments of system rules by all users.

Additionally, in the future, VA will consider whether it will be helpful or necessary to add provisions to VA's standards of conduct maintained at 38 CFR 14.632 as further safeguards. In advocating for systems access for individuals who assist in the representation of claimants, ten commenters pointed out that 38 U.S.C. 5904(a)(2) instructs VA to prescribe in regulations "qualifications and standards of conduct" consistent with the American Bar Association's Model Rules of Professional Conduct (Model Rules) and asserted that the Model Rules contemplate the use of paralegals and other support staff and charge attorneys with supervising responsibility. Although VA does not believe that the Model Rules must control VA's policy decisions on systems access management and accountability, VA does recognize their value as a way to ensure that individuals who practice before VA do so in a responsible and ethical manner or risk losing their VA accreditation.

VA amends 38 CFR 1.600 through 1.603 to, as proposed, confirm its policy that individuals who are accredited by VA pursuant to 38 CFR 14.629 as an attorney, agent, or representative of a VA-recognized VSO may be granted direct access privileges to specific VA IT systems. However, based on the comments received, VA further amends those regulations beyond the proposed rule to allow similar access to some staff members who are affiliated with recognized VSOs and VA-accredited attorneys or claims agents. In addition, within those VA IT systems: (1) VA-accredited VSO representatives will be permitted to access the records of claimants for whom their VSO holds POA pursuant to 38 CFR 14.631; (2) VA-accredited attorneys and agents will be permitted to access the records for claimants for whom they hold the POA; and (3) in some instances, the users—including VA accredited attorneys and agents, their support staff, and the support staff of VSOs—who receive systems access will be able to view records for claimants for whom the users may not directly hold the POA as long as the users are affiliated with the individual or recognized VSO that does

hold the POA and, in the case of an attorney or agent, the claimants represented by that individual have provided their consent to such access on the VA Form 21–22a, *Appointment of Individual as Claimant's Representative*.

Additionally, VA is expanding the provision of direct access privileges to specific VA IT systems to qualifying individuals providing representation under 38 CFR 14.630 of this chapter pursuant to special authority granted by VA's General Counsel to represent more than one claimant. Section 14.630 permits any person complying with the regulation to prepare, present, and prosecute one claim. But, unless an exception is granted by VA's General Counsel under § 14.630(b), such representation may be provided only one time. An exception to this one-time limitation may be granted by the General Counsel in unusual circumstances. To help facilitate responsible, qualified representation by individuals authorized to practice before VA under this special authority, we are revising the proposed amendments to 38 CFR 1.600 through 1.603 to permit systems access to individuals to whom the General Counsel has granted such an exception. VA believes that permitting the possibility of systems access to qualifying individuals with such an authorization would be consistent with the purpose of this rulemaking.

In revising the proposed language to accommodate systems access for qualifying support staff and individuals authorized by the General Counsel under § 14.630, VA has modified proposed § 1.600(b)(1) by removing the reference to an attorney, agent, or representative of a recognized VSO “who is accredited pursuant to part 14 of this chapter.” This does not mean that access will be provided to individuals in those categories who are not accredited. The requirement for accreditation as a prerequisite for individuals in those categories is still contained under qualifications for access in amended § 1.601(a). This is because the statement in § 1.600(b)(1) that VA will provide access only to the categories of attorney, agent, representative of a recognized VSO, support-staff person, or individual authorized by the General Counsel under § 14.630 of this chapter is qualified by the rest of the paragraph “who is approved to access VA IT systems under §§ 1.600 through 1.603.”

VA choosing to allow additional individuals to access specific VA IT systems and to broaden the access permitted within the VA IT systems to individuals who are affiliated with the

accredited individual or recognized VSO that holds the POA means that the individual or VSO holding the POA will have heightened responsibilities that extend further than just their own individual access, in terms of ensuring the confidentiality, integrity, and availability of the information that is stored, processed, and transmitted by VA within its systems. Specifically, VA has amended 38 CFR 1.603(c)(7)(ii) to provide that if the access of an affiliated support-staff person of an attorney or agent is revoked, VA will consider whether to refer the matter to VA's Office of General Counsel for potential inquiry into the principal individual's conduct or competence, pursuant to 38 CFR 14.633.

VA proposed the removal of the note to current 38 CFR 14.629 to clarify policy. The note that follows current 38 CFR 14.629 states that a legal intern, law student, and paralegal, as well as VSO support staff, “may qualify for read-only access to pertinent Veterans Benefits Administration automated claims records” under 38 CFR 1.600 through 1.603. Although VA prevailed in recent litigation concerning the meaning of the note and is continuing with the removal of the note, VA believes the changes from the proposed rule throughout §§ 1.600–1.603 to expand access and privileges satisfy the commenters concerns about systems access for the categories of individuals contemplated by the note.

Finally, while revising the amendatory language of the proposed rule, VA recognized a typographical error in the introductory paragraph of current § 1.600(d). VA is correcting that error by changing “14.603” to “1.603”.

#### **B. Comments Concerning Applicability to Various VA IT Systems**

VA received five comments discussing access to various VA business applications for electronic claims processing, such as the Veterans Benefits Management System (VBMS), Caseflow, Share, and Compensation and Pension Record Interchange (CAPRI). Because all these applications may provide information regarding the current status of a claim or appeal but are systems with significant differences in functionality and underlying purpose—for example, VBMS is a document repository, other systems, such as Share, are not—questions arise regarding to which applications this rule governs access.

VA has revised language proposed in § 1.600(a)(1) that referred to access to “[VBA IT] systems” to refer instead to “specific VA [IT] systems” (emphasis added) to permit VA to provide access

to the electronic claims folder as it specifically decides. VA had proposed removing references to specific systems and instead described affected IT systems more generally to “ensure VA's regulations stay current regardless of future IT developments and to allow VA flexibility to provide access to only those IT systems which are necessary to providing representation while minimizing risk to IT system integrity and privacy.” 85 FR at 9437. However, although VA has in recent years successfully defended in court its ability to determine systems access under the current regulations, the wide range of systems discussed by the commenters made VA concerned that in future litigation a court could have found the proposed language “[VBA's] electronic information technology (IT) systems that contain information regarding the claimants whom they represent before VA” unambiguous and included a specific system to which VA did not intend, or want, to provide access.

In the introductory text of paragraph (b), VA has identified the specific systems VBMS and Caseflow (the eFolder Express and Queue products) to which VA will provide access. VA will provide access to VBMS because that was the current IT system VA contemplated in the proposed rule. See 85 FR at 9436 (noting that the rulemaking was being done in part “to provide increased access to claimant's records” in VBMS and that “a VA-accredited attorney [had] petitioned VA to initiate a rulemaking for purposes of clarifying whether attorney support staff could gain access to VBMS in the same manner as the attorney of record in the claim”); see also *Carpenter v. McDonough*, 34 Vet. App. 261 (2021) (discussing, among other things, the petition for rulemaking, the proposed rule, and numerous arguments advocating for VBMS access for unaccredited paralegals under the existing regulations).

VA will provide access to the eFolder Express product of Caseflow because VA recognizes that the functionality of eFolder Express is directly related to a claimant's VBMS eFolder. The Caseflow eFolder Express product permits downloading of all the files in a claimant's VBMS eFolder in chronological order by date of document receipt with the most recent date at the top of the list. Caseflow is a Board of Veterans' Appeals (Board) IT system, not a VBA IT system (as contemplated in the proposed rule), but multiple commenters indicated that attorneys have been provided access to Caseflow products, and one commenter specifically advocated for VA to provide

access to eFolder Express. Also, although the proposed rule only proposed permitting access to VBA IT systems, the proposed rule did refer to Caseflow. 85 FR at 9436 (“Other systems, such as Caseflow, are not document repositories, but may provide information regarding the current status of the claim or appeal, such as whether it is pending the development of evidence, pending a decision, etc.”). VA believes that providing access to eFolder Express matches VA’s goals in providing access to VBMS. Moreover, providing access to eFolder Express ensures that practitioners will not be overly reliant on VA’s systems (e.g., such as by treating the records accessed through VA systems but not downloaded as their own records). VA will also provide access to Queue, another Caseflow product mentioned by one of the commenters, which provides information regarding the status of some appeals, because providing such access also matches VA’s goals in providing access to VBMS.

VA has specified the only systems to which access will be granted under these regulations. Systems to which VBA does not have administrative rights, such as CAPRI, which was mentioned by one of the commenters, are not included. (Notably, although Caseflow is a Board IT system, VBA personnel have administrative rights for providing access.) Further, although there are additional systems that VBA does administer, VA is only providing access to VBMS and the Caseflow products eFolder Express and Queue because other systems provide substantially duplicative information and any gaps are being evaluated for migration to VBMS. For example, VBA will not give access to the Share application. One commenter indicated that they use Share to review payments and ensure clients receive proper payment amounts. This information is now available in VBMS rendering the Share application redundant.

Finally, although proposed § 1.600(a)(1) had only referred to providing access to claimant records, VA is further revising § 1.600(a)(1) to clarify that qualifying individuals may obtain access to basic information regarding the status of claims or appeals in addition to (read-only) access to claimants’ records. VA is making this change because, as several of the commenters noted, VBMS does provide some basic information regarding the status of claims or appeals. Likewise, VA has modified the language proposed in § 1.602(a) to add a reference to “obtain[ing] basic claims status information.”

### **C. Comments Concerning § 1.601—Qualifications for Access and § 1.602—Utilization of Access**

VA received one comment stating that the provision in proposed 38 CFR 1.601(a)(2) regarding a background suitability investigation for issuance of a personal identity verification (PIV) card was not necessary for attorneys who are members in good standing of a State bar because these individuals have already met a State’s character and fitness requirements. VA declines to exclude attorneys in good standing from the requirement for a background investigation as part of the qualifications for systems access under the final rule. VA is required to implement the use of PIV cards for logistical access to VA networks and information systems. See Homeland Security Presidential Directive-12. In accordance with Office of Management and Budget (OMB) guidance, VA must ensure the initiation of a background investigation and more specifically, either a National Agency Check with Written Inquiries or one that is at least equivalent. See 44 U.S.C. 3554; OMB Circular A-130, *Managing Information as a Strategic Resource*. To comply with OMB’s guidance and meet the specific background criteria, VA is unable to accept certificates of good standing as a substitute for conducting its own suitability investigation.

The same commenter also disagreed with the provision in proposed 38 CFR 1.602(c)(1) allowing VA to inspect computers including hardware and software utilized to obtain systems access. This commenter suggested adding safeguards to the provision to limit the scope and the basis of VA’s ability to inspect privately-owned equipment containing confidential information. This inspection provision is not a new requirement but part of the current regulation and its predecessor since being promulgated in 1994. See 59 FR 47082, 47084–85 (Sept. 14, 1994). Moreover, the requirement to permit such inspection is embedded in the information security requirements to which VA must adhere (identified in the proposed rule, see 85 FR at 9436) and applies to anyone, whether an employee or non-employee, with access to VA IT systems. Its purpose is to protect the integrity of the network and the sensitive information of Veterans, so VA plans no changes to this long-standing policy and subsection based on the comment.

There is no law that requires VA to provide claimants’ representatives or their support staff access to VA IT systems, and there is no expectation of

privacy when accessing VA IT systems. To gain access to VA-specific IT systems, the applicant must agree to general rules of behavior. These rules acknowledge the right of authorized IT personnel to periodically inspect devices, systems, or software used to obtain access to VA’s network. They also include the ability of VA to periodically inspect a remote location for compliance with required security requirements. Approval of the hardware and software ensures the necessary security for systems access. Approval of the location ensures that access is only from the non-VA-employee’s customary and usual or primary place of business, and not from other locations, which might place confidential information at risk of exposure. To properly oversee access activities that provide for the security of the data and systems, VA may, without notice, inspect systems and monitor access activities. VA employs a team of network security experts to monitor and safeguard its systems and databases. Therefore, VA will not change proposed § 1.602(c)(1) based on the comment.

### **D. Comments Concerning § 1.603—Revocation and Reconsideration**

Two commenters commented on the revocation and reconsideration process set forth in 38 CFR 1.603. Both commenters stated that the process should include notice and an opportunity to be heard before the revocation of systems access and should specify a time frame for VA’s decision on reconsideration. One of these commenters also stated that the level of detail specified for the reconsideration decision should be included in the initial final decision. The other commenter recommended that VA provide a more robust procedure for appealing an adverse decision by providing specific standards for what factors are analyzed in the reconsideration process and how this process would work in practicality.

VA has carefully considered these comments, particularly in the context of the existing regulation and proposed amendments. Notably, the proposed rule would have eliminated current § 1.603’s provision of notice of a proposed revocation but retained, in proposed § 1.603(d), VA’s ability to suspend an individual’s systems access if there were exigent circumstances. That combination is somewhat incongruous. VA believes the exigent circumstances provision provides sufficient protection for VA systems and the data therein if VA determines that there is a credible risk of harm. Therefore, VA can provide notice of a

proposed revocation and permit an optional response as requested by the commenters, albeit, subject to the possibility on an immediate suspension of systems access under the exigent circumstances provision in paragraph (d), which specifies that the immediate suspension may take place prior to any determination on the merits of a proposed revocation. Accordingly, VA has added language to provide in paragraph (c)(1) that VA will generally notify the attorney, agent, representative of a recognized VSO, or individual authorized by the General Counsel under 38 CFR 14.630 of the proposed denial or revocation and allow 30 days for an optional response. As suggested by one of the commenters, VA has also added language, in paragraph (c)(2), providing that the initial decision will describe in detail the facts found and state the reasons for VA's final decision, matching in pertinent aspects the content proposed for any decision on reconsideration. VA declines the commenters' request to add a time frame for decisions on access. VA cannot predict the time it will take to issue a decision because that will vary based on the variety of facts and circumstances of each particular case. But VA believes that adding the provision for a proposed notice of revocation fairly addresses some of the concern inherent in the commenters' request that VA specify a time frame for the decision on reconsideration. Under the proposed regulation, the first opportunity to respond to a revocation of access was in the reconsideration phase, likely triggering the commenters' concern about a time frame for a VA decision based on that response. Now, there will be an opportunity to respond to a proposed revocation prior to further VA action unless the exigent circumstances provision applies. (In the exigent circumstances provision, VA has also added an opportunity to respond, similar to language in current § 1.603's exigent circumstances provision but excluded from proposed § 1.603(d).) Likewise, VA believes this change makes the revocation process generally "more robust" as urged by one of the commenters. Under the current regulation, there is a proposed revocation but no reconsideration of a final decision. Under the proposed regulation, there was no proposed revocation. Under the amended regulation, there will be a revocation proposal before further action by VA unless the exigent circumstances provision applies, a decision, and the opportunity for reconsideration of a revocation. As to the commenter's

specific description of a more robust procedure—providing specific standards for what factors are analyzed in the reconsideration process and how this process would work in practicality—VA has also added, in paragraph (c)(2), a standard of proof, the preponderance of the evidence, for the decisions. VA is not making any other changes in response to the commenter's suggestion for further specification because that specification already exists in other parts of the regulations. A revocation or denial of systems access is necessarily premised on a failure to meet a requirement or abide by a rule.

#### **E. Comments Outside the Scope of the Rule**

One commenter requested clarification on whether the proposed amendments could be interpreted as prohibiting VSO support staff from receiving VA network access altogether for those organizations co-located with a VA regional office. The commenter asked VA to include a statement in this rulemaking confirming that co-located administrative support staff for VSOs will continue to be able to utilize basic VA IT functionality. This rulemaking is limited in scope and does not apply to or restrict the basic IT functionality currently provided to administrative support staff for VSOs, co-located within VA regional offices. Therefore, VA made no changes in response to this comment.

One commenter suggested a minimum of thirteen months of incarceration as a penalty for mishandling a claimant's personal information. While VA understands the commenter's desire to deter such misconduct, this comment refers to criminal provisions that are not included in this rulemaking and, therefore, cannot be addressed by this action.

#### **Executive Orders 12866 and 13563**

Executive Orders 12866 and 13563 direct agencies to assess the costs and benefits of available regulatory alternatives and, when regulation is necessary, to select regulatory approaches that maximize net benefits (including potential economic, environmental, public health and safety effects, and other advantages; distributive impacts; and equity). Executive Order 13563 (Improving Regulation and Regulatory Review) emphasizes the importance of quantifying both costs and benefits, reducing costs, harmonizing rules, and promoting flexibility. The Office of Information and Regulatory Affairs has determined that this rule is not a significant regulatory action under

Executive Order 12866. The Regulatory Impact Analysis associated with this rulemaking can be found as a supporting document at [www.regulations.gov](http://www.regulations.gov).

#### **Regulatory Flexibility Act**

The Secretary hereby certifies that the adoption of this final rule will not have a significant economic impact on a substantial number of small entities as they are defined in the Regulatory Flexibility Act (5 U.S.C. 601–612). This final rule might have an insignificant economic impact on an insubstantial number of small entities, generally, law firms that have individual attorneys who are accredited by VA for purposes of representing VA benefit claimants. VA believes the impact to be minimal because access to VA systems is optional and not a prerequisite to representing any claimant before VA. Therefore, under 5 U.S.C. 605(b), the initial and final regulatory flexibility analysis requirements of 5 U.S.C. 603 and 604 do not apply.

#### **Unfunded Mandates**

The Unfunded Mandates Reform Act of 1995 requires, at 2 U.S.C. 1532, that agencies prepare an assessment of anticipated costs and benefits before issuing any rule that may result in the expenditure by State, local, and tribal governments, in the aggregate, or by the private sector, of \$100 million or more (adjusted annually for inflation) in any one year. This final rule will have no such effect on State, local, and tribal governments, or on the private sector.

#### **Paperwork Reduction Act**

This final rule contains no provisions constituting a collection of information under the Paperwork Reduction Act of 1995 (44 U.S.C. 3501–3521).

#### **Assistance Listing**

There are no assistance listing program numbers and titles for this rule.

#### **Congressional Review Act**

Pursuant to Subtitle E of the Small Business Regulatory Enforcement Fairness Act of 1996 (known as the Congressional Review Act), 5 U.S.C. 801 *et seq.*, the Office of Information and Regulatory Affairs designated this rule as not a major rule, as defined by 5 U.S.C. 804(2).

#### **List of Subjects**

##### *38 CFR Part 1*

Administrative practice and procedure, Archives and records, Cemeteries, Claims, Courts, Crime, Flags, Freedom of information, Government contracts, Government

employees, Government property, Infants and children, Inventions and patents, Parking, Penalties, Postal service, Privacy, Reporting and recordkeeping requirements, Seals and insignia, Security measures, Wages.

### 38 CFR Part 14

Administrative practice and procedure, Claims, Courts, Foreign relations, Government employees, Lawyers, Legal services, Organization and functions (Government agencies), Reporting and recordkeeping requirements, Surety bonds, Trusts and trustees, Veterans.

### Signing Authority

Denis McDonough, Secretary of Veterans Affairs, approved this document on June 6, 2022, and authorized the undersigned to sign and submit the document to the Office of the Federal Register for publication electronically as an official document of the Department of Veterans Affairs.

### Luvenia Potts,

*Regulations Development Coordinator, Office of Regulation Policy & Management, Office of General Counsel, Department of Veterans Affairs.*

For the reasons set forth in the preamble, VA amends 38 CFR parts 1 and 14 as follows:

## PART 1—GENERAL PROVISIONS

■ 1. The authority citation for part 1, is revised to read as follows:

**Authority:** 31 U.S.C. 3711(e); 38 U.S.C. 501, 5701(g) and (i); 38 U.S.C. 5320. 38 U.S.C. 1751–1754 and 7331–7334. Sections 1.500–1.527 issued under 72 Stat. 1114, 1236, as amended; 38 U.S.C. 501, 5701. Sections 1.600–1.603 also issued under 38 U.S.C. 5721–5728.

■ 2. Amend the undesignated center heading preceding § 1.600 by removing the word “Remote”.

■ 3. Amend § 1.600 by:

■ a. Revising paragraph (a)(1).

■ b. Amending paragraph (a)(2) by removing “claimants’ representatives” and adding in its place “attorneys, agents, representatives of a VA-recognized service organization, affiliated support-staff personnel, and individuals authorized by the General Counsel under § 14.630 of this chapter”.

■ c. Revising paragraph (a)(3).

■ d. Revising paragraphs (b), (c), and (d).

The revisions read as follows:

### § 1.600 Purpose.

(a) \* \* \*

(1) When, and under what circumstances, VA will grant attorneys, agents, representatives of a VA-

recognized service organization, affiliated support-staff personnel, and individuals authorized by the General Counsel under § 14.630 of this chapter the ability to access records and basic claims status information through specific VA electronic information technology (IT) systems that contain information regarding the claimants whom they represent or assist in representing before VA;

\* \* \* \* \*

(3) The bases and procedures for denial or revocation of access privileges to VA IT systems of an attorney, agent, representative of a VA-recognized service organization, affiliated support-staff person, or individual authorized by the General Counsel under § 14.630 of this chapter for violating any of the requirements for access.

(b) VA will provide access to specific VA IT systems, the Veterans Benefit Management System (VBMS) and the Caseflow products Queue and eFolder Express, under the following conditions:

(1) Only to an attorney, agent, representative of a VA-recognized service organization, affiliated support-staff person, or individual authorized by the General Counsel under § 14.630 of this chapter who is approved to access VA IT systems under §§ 1.600 through 1.603;

(2)(i) For a representative or affiliated support-staff person of a VA-recognized service organization, only to the records of VA claimants who appointed the service organization as the organization of record to provide representation on their claims,

(ii) For an attorney or agent, only to the records of VA claimants who either appointed the attorney or agent as the attorney or agent of record on their claims or appointed an attorney or agent employed by the same legal services office as the attorney or agent of record and consented to affiliated access on VA Form 21–22a, “Appointment of Individual as Claimant’s Representative,”

(iii) For an individual authorized by the General Counsel under § 14.630 of this chapter, only to the records of VA claimants who appointed the individual to provide representation on their claims, or

(iv) For a support-staff person working under the direct supervision of an accredited attorney or agent only to the records of VA claimants who appointed the attorney or agent as the attorney or agent of record on their claims and consented to affiliated access on VA Form 21–22a, “Appointment of Individual as Claimant’s Representative”;

(3) Solely for the purpose of representing or assisting in the representation of the individual claimant whose records are accessed in a claim for benefits administered by VA; and

(4) On a read-only basis, an attorney, agent, representative of a VA-recognized service organization, affiliated support-staff person, or individual authorized by the General Counsel under § 14.630 of this chapter authorized to access VA IT systems under §§ 1.600 through 1.603 will not be permitted to modify the data, to include modifying any existing records. However, such an attorney, agent, representative of a VA-recognized service organization, or individual authorized by the General Counsel under § 14.630 of this chapter may upload documents as permitted by VA IT policy regarding submittal of new documents.

(c) Privileges to access VA IT systems may be granted by VA only for the purpose of accessing a represented claimant’s electronically stored records pursuant to applicable privacy laws and regulations, and as authorized by a claimant’s power of attorney under § 14.631 of this chapter.

(d) Sections 1.600 through 1.603 are not intended to, and do not:

(1) Waive the sovereign immunity of the United States;

(2) Create, and may not be relied upon to create, any right or benefit, substantive or procedural, enforceable at law against the United States or VA; or

(3) Create or establish a right to electronic access.

■ 4. Revise § 1.601 to read as follows:

### § 1.601 Qualifications for access.

(a)(1) An applicant for access to VA IT systems for the purpose of providing representation or assisting in representation must be:

(i) A representative of a VA-recognized service organization who is accredited by VA under § 14.629(a) of this chapter through a service organization and whose service organization holds power of attorney for one or more claimants under § 14.631 of this chapter;

(ii) An attorney or agent who is accredited by VA under § 14.629(b) of this chapter and who:

(A) holds power of attorney for one or more claimants under § 14.631 of this chapter or

(B) is authorized to assist in the representation of one or more claimants as an associate attorney or agent employed by the same legal services office as the attorney or agent of record;

(iii) An unaccredited support-staff person, including a legal intern, law

student, or paralegal, working under the direct supervision of an accredited attorney or agent who has been designated to provide representation to one or more claimants under § 14.631(a) of this chapter or an accredited representative of a VA-recognized service organization designated to provide representation to one or more claimants under § 14.631(a); or

(iv) An individual authorized by the General Counsel under § 14.630 of this chapter to represent, without VA accreditation, more than one claimant and holding power of attorney for one or more claimants under § 14.631 of this chapter.

(2) To qualify for access to VA IT systems, the applicant must comply with all security requirements deemed necessary by VA to ensure the integrity and confidentiality of the data and VA IT systems, which may include passing a background suitability investigation for issuance of a personal identity verification badge.

(3) VA may deny access to VA IT systems if the requirements of paragraphs (a)(1) or (2) of this section are not met.

(b) The method of access, including security software and work-site location of the attorney, agent, representative of a VA-recognized service organization, affiliated support-staff person, or individual authorized by the General Counsel under § 14.630 of this chapter, must be approved in advance by VA.

(c) Each attorney, agent, representative of a VA-recognized service organization, affiliated support-staff person, or individual authorized by the General Counsel under § 14.630 of this chapter approved for access must complete, sign, and return a notice provided by VA. The notice will specify any applicable operational and security requirements for access, in addition to the applicable VA Rules of Behavior, and an acknowledgment that the breach of any of these requirements is grounds for revocation of access.

■ 5. Revise § 1.602 to read as follows:

**§ 1.602 Utilization of access.**

(a) Once VA issues to an attorney, agent, representative of a VA-recognized service organization, affiliated support-staff person, or individual authorized by the General Counsel under § 14.630 of this chapter the necessary logon credentials to obtain basic claims status information and read-only access to the VA records regarding the claimants represented, access will be exercised in accordance with the following requirements. The attorney, agent, representative of a VA-recognized service organization, support-staff

person, or individual authorized by the General Counsel under § 14.630 of this chapter:

(1) Will electronically access VA records through VA IT systems only by the method of access approved in advance by VA;

(2) Will use only his or her assigned logon credentials to obtain access;

(3) Will not reveal his or her logon credentials to anyone else, or allow anyone else to use his or her logon credentials;

(4) Will access via VA IT systems only the records of claimants whom he or she represents or is authorized to assist in representing;

(5) Will access via VA IT systems a claimant's records solely for the purpose of representing or assisting in the representation of that claimant in a claim for benefits administered by VA;

(6) Is responsible for the security of the logon credentials and, upon receipt of the logon credentials, will destroy the hard copy so that no written or printed record is retained;

(7) Will comply with all security requirements VA deems necessary to ensure the integrity and confidentiality of the data and VA IT systems; and

(8) Will, if accredited or authorized by the General Counsel under § 14.630 of this chapter, comply with each of the standards of conduct for accredited individuals prescribed in § 14.632 of this chapter.

(b)(1) A VA-recognized service organization shall ensure that all its representatives and support-staff personnel provided access in accordance with these regulations receive annual training approved by VA on proper security or annually complete VA's Privacy and Security Training.

(2) An attorney, agent, affiliated support-staff person of an attorney or agent, or individual authorized by the General Counsel under § 14.630 of this chapter who is provided access in accordance with these regulations will annually acknowledge review of the security requirements for the system as set forth in these regulations, VA's Rules of Behavior, and any additional materials provided by VA.

(c) VA may, at any time without notice:

(1) Inspect the computer hardware and software utilized to obtain access and their location;

(2) Review the security practices and training of any attorney, agent, representative of a VA-recognized service organization, support-staff person, or individual authorized by the General Counsel under § 14.630 of this chapter provided access in accordance with these regulations; and

(3) Monitor the access activities of an attorney, agent, representative of a VA-recognized service organization, support-staff person, or individual authorized by the General Counsel under § 14.630 of this chapter. By applying for and exercising the access privileges under §§ 1.600 through 1.603, the individual expressly consents to VA monitoring access activities at any time for the purpose of auditing system security.

■ 6. Amend § 1.603 by:

■ a. Revising the section heading.

■ b. Revising paragraph (a).

■ c. Revising paragraphs (b) introductory text and (b)(2).

■ d. Removing paragraph (b)(3).

■ e. Redesignating paragraph (b)(4) as (b)(3) and revising the newly redesignated (b)(3).

■ f. Redesignating paragraph (b)(5) as (b)(4) and revising the newly redesignated (b)(4).

■ g. Redesignating paragraph (b)(6) as (b)(5) and revising the newly redesignated (b)(5).

■ h. Revising paragraph (c).

■ i. Removing paragraph (d).

■ j. Redesignating paragraph (e) as (d) and revising the newly redesignated (d).

The revisions read as follows:

**§ 1.603 Revocation and reconsideration.**

(a)(1) VA may revoke access of an attorney, agent, representative of a VA-recognized service organization, affiliated support-staff person, or individual authorized by the General Counsel under § 14.630 of this chapter to a particular claimant's records because the principal individual or organization no longer represents the claimant, and, therefore, the claimant's consent is no longer in effect.

(2) VA may revoke access of a previously affiliated attorney or agent to a particular claimant's records because the attorney or agent is no longer affiliated with the principal individual, and, therefore, the claimant's consent is no longer in effect.

(3) VA may revoke access privileges of a previously affiliated support-staff person to all claimants' records because the support-staff person is no longer affiliated with the principal individual or VA-recognized service organization, and, therefore, the claimants' consent is no longer in effect.

(b) VA may revoke the access privileges of an attorney, agent, representative of a VA-recognized service organization, affiliated support-staff person, or individual authorized by the General Counsel under § 14.630 of this chapter, either to an individual claimant's records or to all claimants' records via the VA IT systems, if the

individual, or, additionally in the case of the affiliated support-staff personnel of an attorney or agent, the principal individual:

\* \* \* \* \*

(2) Accesses or attempts to access data for a purpose other than representation or assistance in the representation of an individual claimant;

(3) Accesses or attempts to access data of a claimant whom he, she, or the VA-recognized service organization neither represents nor is authorized to assist in representing;

(4) Accesses or attempts to access a VA IT system by a method that has not been approved by VA; or

(5) Modifies or attempts to modify data in a VA IT system without authorization.

(c)(1) To initiate the process for denial of access under § 1.601(a)(3) or revocation of access under paragraph (b) of this section, VA will notify the attorney, agent, representative of a VA-recognized service organization, support-staff person, or individual authorized by the General Counsel under § 14.630 of this chapter of the proposed denial or revocation. If VA is initiating the process to deny or revoke access privileges for a representative of a VA-recognized service organization or any support-staff person, VA will notify the service organization(s) through which the representative is accredited, or the employer of the support-staff person, of the proposal. If VA is initiating the process to revoke access privileges for an attorney or agent based on conduct related to the attorney's or agent's authorized assistance in the representation of one or more claimants, VA will notify the claimants' attorney or agent of record of the revocation proposal. VA's notice will include the procedures applicable to the proposed denial or revocation, including instructions for submitting an optional response and identification of the official making the final decision. VA will allow 30 days for an optional response to the proposal.

(2) After considering any timely-received response, VA will issue a final decision based on a preponderance of the evidence. The decision will describe in detail the facts found and state the reasons for VA's final decision. If VA denies or revokes access privileges for a representative of a VA-recognized service organization or any support-staff person, VA will notify the service organization(s) through which the representative is accredited, or the employer of the support-staff person, of the denial or revocation of access. If VA revokes access privileges for an attorney

or agent based on conduct related to the attorney's or agent's authorized assistance in the representation of one or more claimants, VA will notify the claimants' attorney or agent of record of the revocation of access.

(3) The attorney, agent, representative of a VA-recognized service organization, support-staff person, or individual authorized by the General Counsel under § 14.630 of this chapter may request reconsideration of a denial or revocation of access by submitting a written request to VA. VA will consider the request if it is received by VA not later than 30 days after the date that VA notified the attorney, agent, representative of a VA-recognized service organization, support-staff person, or individual authorized by the General Counsel under § 14.630 of this chapter of its decision.

(4) The attorney, agent, representative of a VA-recognized service organization, support-staff person, or individual authorized by the General Counsel under § 14.630 of this chapter may submit additional information not previously considered by VA, provided that the additional information is submitted with the written request and is pertinent to the prohibition of access.

(5) VA will close the record regarding reconsideration at the end of the 30-day period described in paragraph (c)(3) of this section and furnish the request, including any new information submitted by the attorney, agent, representative of a VA-recognized service organization, support-staff person, or individual authorized by the General Counsel under § 14.630 of this chapter to the Director of the VA regional office or center with jurisdiction over the final decision.

(6) VA will reconsider access based upon a review of the information of record as of the date of its prior denial or revocation, with any new information submitted with the request. The decision will:

(i) Identify the attorney, agent, representative of a VA-recognized service organization, support-staff person, or individual authorized by the General Counsel under § 14.630 of this chapter,

(ii) Identify the date of VA's prior decision,

(iii) Describe in detail the facts found as a result of VA's review of its decision with any new information submitted with the reconsideration request, and

(iv) State the reasons for VA's final decision, which may affirm, modify, or overturn its prior decision.

(7) VA will provide notice of its final decision on access to:

(i) The attorney, agent, representative of a VA-recognized service organization, support-staff person, or individual authorized by the General Counsel under § 14.630 of this chapter requesting reconsideration, and

(ii) if the conduct that resulted in denial or revocation of the authority of an attorney, agent, representative of a VA-recognized service organization, support-staff person, or individual authorized by the General Counsel under § 14.630 of this chapter to access VA IT systems merits potential inquiry into the individual's conduct or competence, or in the case of an affiliated support-staff person of an attorney or agent, the principal individual's conduct or competence, pursuant to § 14.633 of this chapter, the VA regional office or center of jurisdiction will immediately inform VA's Office of General Counsel in writing of the fact that it has denied or revoked the individual's access privileges and provide the reasons why.

(d) VA may immediately suspend access privileges prior to any determination on the merits of a proposed revocation where VA determines that such immediate suspension is necessary to protect, from a reasonably foreseeable compromise, the integrity of the system or confidentiality of the data in VA IT systems. However, in such case, VA shall offer the individual an opportunity to respond to the charges that led to the immediate suspension and the proposed revocation after the temporary suspension.

#### **PART 14—LEGAL SERVICES, GENERAL COUNSEL, AND MISCELLANEOUS CLAIMS**

■ 7. The authority citation for part 14 continues to read as follows:

**Authority:** 5 U.S.C. 301; 28 U.S.C. 2671–2680; 38 U.S.C. 501(a), 512, 515, 5502, 5901–5905; 28 CFR part 14, appendix to part 14, unless otherwise noted.

##### **§ 14.629 [Amended]**

■ 8. Amend § 14.629 by removing the Note.

[FR Doc. 2022–13312 Filed 6–23–22; 8:45 am]

**BILLING CODE 8320–01–P**