United States Court of Appeals for the Federal Circuit

MILITARY-VETERANS ADVOCACY,
Petitioner

v.

SECRETARY OF VETERANS AFFAIRS,
Respondent

2023-1413

Petition for review pursuant to 38 U.S.C. Section 502.

Decided: March 6, 2025

WILLIAM MILLIKEN, Sterne Kessler Goldstein & Fox PLLC, Washington, DC, argued for petitioner. Also represented by PAIGE CLOUD, MICHAEL E. JOFFRE; JOHN B. WELLS, Law Office of John B. Wells, Slidell, LA.

ERIC LAUFGRABEN, Commercial Litigation Branch, Civil Division, United States Department of Justice, Washington, DC, argued for respondent. Also represented by BRIAN M. BOYNTON, MARTIN F. HOCKEY, JR., PATRICIA M. MCCARTHY; CHRISTA A. SHRIBER, JONATHAN ELLIOTT TAYLOR, NICHOLAS XANTHAKOS, Office of General Counsel, United States Department of Veterans Affairs, Washington, DC.

Before MOORE, *Chief Judge*, STOLL, *Circuit Judge*, and GILSTRAP, *Chief District Judge*.[1]

MOORE, *Chief Judge*.

Military-Veterans Advocacy (MVA) filed a petition for review pursuant to 38 U.S.C. § 502, challenging *Individuals Using the Department of Veterans Affairs' Information Technology Systems to Access Records Relevant to a Benefit Claim*, 87 Fed. Reg. 121, 37744 (June 24, 2022) (Final Rule). Specifically, MVA challenges the validity of 38 C.F.R. § 1.601(a)(2), which requires users of Veterans Affairs' (VA) Information Technology (IT) systems to potentially pass "a background suitability investigation" (the Background Check Provision), and 38 C.F.R. § 1.602(c)(1), which permits the VA to, "at any time without notice," "inspect the computer hardware and software utilized to obtain access to VA IT systems and their location" (the Inspection Provision). Because we hold the VA has authority to promulgate the Background Check Provision, but not the Inspection Provision, we grant-in-part and deny-in-part the petition and set aside 38 C.F.R. § 1.602(c)(1) of the Final Rule.

BACKGROUND

Title 38 of the United States Code establishes benefits for veterans who suffer from service-connected disabilities. In pursuit of these benefits, veterans may be represented by attorneys, agents, or a VA-recognized organization. 38 U.S.C. § 5904. To represent a veteran, an attorney or agent is provided access to the veteran's claim file. 38 U.S.C. § 5701(b)(1); 38 C.F.R. § 1.577(a). Claim files often include sensitive and confidential information, such as

---

[1] Honorable Rodney Gilstrap, Chief Judge, United States District Court for the Eastern District of Texas, sitting by designation.

the veteran's financial and medical records. Government Br. 5. Claim files can be accessed in three ways: (1) reviewing a paper copy at the VA, (2) requesting an electronic version on a compact disc or thumb drive, or (3) online through two internal VA electronic systems—Veterans Benefits Management System (VBMS) and Caseflow. Since 1994, the VA has permitted accredited individuals to apply for and obtain remote, read-only access to claim files on VBMS and Caseflow.

The VA issued a Notice of Proposed Rulemaking to amend regulations 38 C.F.R. §§ 1.600, 1.601, 1.602, and 1.603, which address user requirements for accessing the VA IT systems. 85 Fed. Reg. 33, 9435 (Feb. 19, 2020). Relevant to MVA's petition are 38 C.F.R. §§ 1.601(a)(2) and 1.602(c)(1). The proposed rule added the following language to 38 C.F.R. § 1.601(a)(2):

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

85 Fed. Reg. at 9440. For 38 C.F.R. § 1.602(c)(1), the proposed rule maintained the prior language:

> (c) VBA may, at any time without notice:
>
> (1) inspect the computer hardware and software utilized to obtain access and their location[.]

85 Fed. Reg. at 9441.

MVA submitted comments in response to the proposed rulemaking. J.A. 1174–83. MVA argued the regulations violated the pro-veteran canon of construction and due

process, and are arbitrary and capricious by placing burdens on attorneys and violating attorney-client privilege. *Id.*

The VA issued the relevant rules as proposed, with the exception of changing "VBA" to "VA," and addressed some of MVA's comments in its Final Rule. 87 Fed. Reg. at 37749–50. For the Background Check Provision, the VA explained attorneys who are in good standing with the bar cannot be excluded from the requirement because the provision is required to implement personal identity verification badges. 87 Fed. Reg. at 37747. For the Inspection Provision, the VA noted the requirement had been in place since 1994 and applies to everyone who wants access to VA IT systems, and there is no law requiring the VA to provide access to the IT systems and no expectation of privacy when accessing the systems. *Id.* The Final Rule issued on June 24, 2022. 87 Fed. Reg. at 37744.

MVA filed a petition for review of the Final Rule, specifically the Background Check and Inspection Provisions. We have jurisdiction pursuant to 38 U.S.C. § 502.

DISCUSSION

I. Standing

Before reaching the merits of MVA's petition, we first determine whether MVA has Article III standing. "[S]tanding is an essential and unchanging part of the case-or-controversy requirement of Article III." *Lujan v. Defs. of Wildlife*, 504 U.S. 555, 560 (1992). For a petitioner to have standing, it must show (1) an "injury in fact," (2) "a causal connection between the injury and the conduct complained of," and (3) a likelihood that "the injury will be 'redressed by a favorable decision.'" *Id.* at 560–61 (quoting *Simon v. E. Ky. Welfare Rts. Org.*, 426 U.S. 26, 38, 43 (1976)). To show standing as an organization, MVA must demonstrate the same requirements. *Military-Veterans*

Advoc. v. Sec'y of Veterans Affs., 7 F.4th 1110, 1129 (Fed. Cir. 2021).

MVA argues it has organizational standing. Pet. 1–3; Reply Br. 5–6. The Government disagrees, arguing MVA cannot show injury-in-fact. Government Br. 20–21. We hold MVA has organizational standing to challenge the Final Rule because MVA demonstrated injury-in-fact.[2]

Injury-in-fact is established by a "concrete and demonstrable injury to the organization's activities." *Havens Realty Corp. v. Coleman*, 455 U.S. 363, 379 (1982). MVA litigates, legislates, and educates on behalf of members of the military and military veterans. Pet. 1–2. In its representation of veterans, MVA uses, or would use if not for the Final Rule, VA IT systems governed by the Final Rule. Add. 4–6; Add. 8–11 (declarations of MVA members).[3] MVA argues the Final Rule frustrates its goal of representing veterans by, for example, requiring its attorneys to use paper copies of client files rather than VBMS and Caseflow and causing its attorneys to lose veteran clients due to lack of VBMS and Caseflow access for failure to comply with the Background Check and Inspection Provisions of the Final Rule. Reply Br. 6; *see also* Add. 2–11. This is more "than simply a setback to the organization's abstract social interests," but a concrete injury-in-fact. *Havens*, 455 U.S. at 379. Because MVA has organizational standing to

---

[2] Because we hold MVA has organizational standing, we need not address whether MVA has associational standing.

[3] MVA moved to file an addendum containing two declarations from its members with the Reply Brief. E.C.F. No. 35. Because the Government did not oppose, *id.* at 2, we granted the motion, E.C.F. 40, and now consider these materials.

challenge 38 C.F.R. §§ 1.601(a)(2) and 1.602(c)(1), we address the merits of MVA's petition.

II. The Final Rule

We have jurisdiction to review the validity of both the rulemaking process and the challenged rules of the VA. *McKinney v. McDonald*, 796 F.3d 1377, 1383 (Fed. Cir. 2015); 38 U.S.C. § 502. We review the agency's action pursuant to 5 U.S.C. § 706(2) to determine whether the action was "arbitrary, capricious, an abuse of discretion, or otherwise not in accordance with law." *Serv. Women's Action Network v. Sec'y of Veterans Affs.*, 815 F.3d 1369, 1374 (Fed. Cir. 2016). In our review, we "look to see whether the agency employed reasoned decisionmaking." *Id.* A challenge to the constitutionality of a regulation is a question of law we review without deference to the agency. *Preminger v. Sec'y of Veterans Affs.*, 517 F.3d 1299, 1311–12 (Fed. Cir. 2008).

A. The Background Check Provision

The Background Check Provision of the Final Rule provides:

> 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.

38 C.F.R. § 1.601(a)(2) (emphasis added). MVA argues the provision exceeds the VA's statutory authority and is not the product of reasoned decision making. MVA Opening Br. 53–61. We do not agree.

The Background Check Provision is within the VA's statutory authority to promulgate regulations regarding information security. The VA cited 38 U.S.C.

§§ 501, 5721–28 as authority for promulgating 38 C.F.R. §§ 1.600–1.603, which includes the Background Check Provision. 87 Fed. Reg. at 37749. Under 38 U.S.C. § 501, the VA, through the Secretary, "has authority to prescribe all rules and regulations which are necessary or appropriate to carry out the laws administered by the Department." The VA is charged with prescribing rules to "establish and maintain a comprehensive Department-wide information security program to provide for the development and maintenance of cost-effective security controls needed to protect Department information, in any media or format, and Department information systems." 38 U.S.C. § 5722(a). The VA, through the Assistant Secretary for Information and Technology, is also responsible for "[e]stablishing, maintaining, and monitoring Department-wide information security policies, procedures, control techniques, training, and inspection requirements as elements of the department information security program," 38 U.S.C. § 5723(b)(1), and "[e]stablishing standards for access to Department information systems by organizations and individual employees, and to deny access as appropriate," 38 U.S.C. § 5723(b)(6). These statutory provisions give the VA the authority to implement security requirements for access to VA IT systems.

The VA's ability to promulgate regulations for IT security is tempered by the very same statute which provides the authority. The Secretary "shall ensure that the Department information security program . . . [p]olicies and procedures [] are based on risk assessments." 38 U.S.C. § 5722(b)(2)(a). The VA conducted and considered risk assessments for VBMS and Caseflow. Government Br. 31; *see, e.g.*, S. Appx. 1 (risk assessment for VBMS Cloud Assessing); *id.* at 46 (risks of remote access from separate devices); *id.* at 48 (vulnerability summary relating to personal identity verification cards). The background check "for issuance of a personal identity verification

badge," 38 C.F.R. § 1.601(a)(2), is based on a risk assessment as required by the statute, 38 U.S.C. § 5722(b)(2)(a).

MVA argues even if the VA has the authority to promulgate the regulation, it is not reasonable because the VA failed to consider its impact on veterans' access to attorneys. MVA Opening Br. 60. MVA argues that attorneys already have background checks pursuant to their bar license and that this additional background check is an unreasonable exercise of VA authority. The Background Check Provision, however, is not directed only to attorneys. Rather than limiting access to VBMS and Caseflow to attorneys, the Final Rule expands access to staff members such as paralegals and administrative support staff. 87 Fed. Reg. at 37745 ("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."). Even if MVA were correct that the attorneys who access the systems already have sufficient background checks, MVA fails to address the government's argument that the additional support staff newly authorized to access these databases would not have had similar background checks. The VA explained the Background Check Provision applies equally to everyone who applies for remote access to VBMS and Caseflow. Government Br. 25. The VA also considered that "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." 87 Fed. Reg. at 37745. The Background Check Provision is therefore grounded in the risk assessment and tethered to the VA's authority in protecting information security and it is the product of reasoned decision making.

B. The Inspection Provision

The Inspection Provision of the Final Rule provides:

> VA may, at any time without notice . . . inspect the computer hardware and software utilized to obtain access and their location.

38 C.F.R. § 1.602(c)(1). MVA argues the provision: (1) is unconstitutional under the Fourth Amendment, (2) exceeds the VA's statutory authority, and (3) is not the product of reasoned decision-making. MVA Opening Br. 20–53. We address each argument in turn.

MVA argues that this inspection provision is an unreasonable search which violates the Fourth Amendment. We may consider only facial challenges, rather than as applied challenges, to regulations. *Preminger*, 517 F.3d at 1308 n.5. With a facial challenge, if any application of the regulation would not violate the Fourth Amendment, we may not set the regulation aside. Here, there are applications of the Inspection Provision that do not violate the Fourth Amendment. For example, MVA agreed at oral argument that the Inspection Provision allows the VA to ensure that a user is accessing the systems from an approved location, and such an inspection would be reasonable.[4] And users expressly agree to the VA Rules of Behavior, which state users do not have any expectation of privacy, will comply with security measures, and agree to inspections to gain access to VA IT systems. J.A. 1948–49. Consent is an exception to the Fourth Amendment's prohibition on unreasonable search and seizures. *See, e.g.*, *Schneckloth v. Bustamonte*, 412 U.S. 218, 219 (1973). Because there are some circumstances where the Inspection Provision does not violate the Fourth Amendment, it is not facially unconstitutional. *See, e.g.*, *United States v. Salerno*, 481 U.S. 739, 745 (1987) ("the challenger must establish that no set

---

[4] *See* Oral Argument at 6:16–58, *available at* https://oralarguments.cafc.uscourts.gov/default.aspx?fl=23-1413_01072025.mp3.

of circumstances exists under which the [regulation] would be valid").

MVA argues the Inspection Provision exceeds the VA's statutory authority. We agree. The provision gives the VA the authority to inspect not only the computer hardware and software used to access the VA IT systems, but also the location where the hardware and software are used. As the regulation is written, this could include the user's home office, entire house, client files, or sensitive personal documents, to name a few examples. The Government agrees that anywhere a user accesses the VA IT systems could be searched, including a user's bedroom in their home. *See* Oral Argument at 35:32–50, 38:03–35. This scope is particularly untethered to the statutory authority because the VA is generally an adverse party to the user of the VA IT system. This is a "markedly different" power than Congress likely envisioned in granting the VA the authority to promulgate information security policies. *Ala. Ass'n of Realtors v. Dep't of Health & Hum. Servs.*, 594 U.S. 758, 764 (2021). VA argues the provision is limited in scope and would not include "rummaging through attorneys' drawers and cabinets." Government Br. 61. But the language of the Inspection Provision is not so limited. Whether the VA chooses to utilize the full scope of the Inspection Provision does not bear on our analysis.

The Inspection Provision also exceeds the VA's statutory authority because it is not based on a risk assessment as required by VA regulations implementing information security policies and procedures. 38 U.S.C. § 5722(b)(2)(a). The VA argues the Inspection Provision is based on the VBMS and Caseflow risk assessments. Government Br. 54–55. But the VA's citations to the risk assessment do not link any risk to confidentiality to computer hardware and software utilized to obtain access to VA IT systems or their location. S. Appx 2; S. Appx 157.

Even if the VA could demonstrate the Inspection Provision is properly grounded in a risk assessment, given the breadth of the provision, it is not the product of reasoned decision making. The VA argues the Inspection Provision is reasonable because it addresses the risk of disclosing sensitive personal information with remote access to VA systems. Government Br. 52; 87 Fed. Reg. at 37747. That may be a reasonable goal, but this record does not demonstrate the VA has a rational basis to promulgate a regulation as broad as the Inspection Provision to effectuate that goal. The VA has not demonstrated that the breadth of the Inspection Provision is required to meet the goals of information security.

CONCLUSION

We have considered the parties' remaining arguments and find them unpersuasive. For the forgoing reasons, we grant-in-part and deny-in-part MVA's petition.

GRANTED-IN-PART AND DENIED-IN-PART

COSTS

Costs to MVA.