STONE BRAVO
OUTPOST LLC
VETERAN-OWNED • KILLEEN, TX

Stone Bravo Outpost LLC
Killeen, Texas

August 1, 2026

ATF Rulemaking Comments
Mail Stop 6N-518, Office of Regulatory Affairs
Enforcement Programs and Services
Bureau of Alcohol, Tobacco, Firearms, and Explosives
99 New York Ave. NE
Washington, DC 20226
ATTN: ATF 1140-AB05

Via electronic submission to the Federal eRulemaking Portal, https://www.regulations.gov

Re: Notice of Proposed Rulemaking
Revising Non-Over-the-Counter Firearms Transaction Requirements
Docket No. ATF-2026-0266; ATF 2025R-26P
RIN 1140-AB05
Federal Register Document No. 2026-09157
91 Fed. Reg. 25,216 (May 8, 2026)
Comment period closes August 6, 2026

Greetings:

Stone Bravo Outpost LLC submits these comments on the above-captioned Notice of Proposed Rulemaking (the "Proposed Rule"). Stone Bravo Outpost LLC is a Texas limited liability company with an interest in the regulatory category addressed by the Proposed Rule.

I. Position

Stone Bravo Outpost LLC supports the Proposed Rule's amendment of 27 C.F.R. § 478.96 to permit federal firearms licensees to conduct non-over-the-counter ("NOTC") transactions subject to the background-check requirements of 18 U.S.C. § 922(t), paired with remote identity proofing of the transferee conforming to the National Institute of Standards and Technology ("NIST") guidelines for Identity Assurance Level 2 — a standard the proposed regulatory text identifies only as the "NIST guidelines," and which Part II.A asks ATF to name by publication and revision. 91 Fed. Reg. at 25,228.

Under proposed § 478.96(c)(3), the CSP-based remote identity verification of the transferee sits alongside the licensee's video conference with the transferee and inspection of the transferee's photo identification document. 91 Fed. Reg. at 25,228. The company does not read that provision as displacing the licensee's own verification, and its comments below proceed on that reading.

II. Requested modifications

The company requests four refinements.

A. Identify the identity standard by publication and revision; do not name a provider

Preserve vendor neutrality. The Proposed Rule's regulatory text does not name any credential service provider ("CSP"), and should not. ATF does name commercial providers, but only in the preamble, and only by way of illustration. The preamble notes that several federal agencies "have implemented IAL2 remote identity proofing," and observes that "[t]he IRS, for example, allows individual taxpayers to create an ID.me account to access IRS-held information requiring identity verification," 91 Fed. Reg. at 25,218, going on to describe the IRS's "video chat agent" process "with an ID.me trusted referee," *id.* at 25,219. The regulatory analysis names ID.me once more as an example of software the public already encounters, "such as by the IRS and ID.me," *id.* at 25,223, and names "Veriff or Sumsub" and "Kantara" only in surveying what the current market charges and who assesses it, *id.* at 25,224. Each of those is an example of an agency implementation or a market observation, not an endorsement of a provider. The regulatory text itself names no provider, and that is the feature worth preserving. Confining provider names to the preamble, as ATF has done, is correct, and the final rule should preserve it. Doing so:

1. permits new providers achieving NIST conformance to participate without further rulemaking;
2. automatically excludes providers that fall out of conformance; and
3. avoids regulatory endorsement of any single private vendor.

Name the standard precisely. The vendor-neutral approach works only if the standard the regulatory text points to is unambiguous, and at present it is not. Proposed § 478.96(c)(3)(ii) requires an independent third party to assess the CSP's remote identity proofing process "as conforming with the National Institute of Standards and Technology (NIST) guidelines for Identity Assurance Level 2 (IAL2)," and to assess the CSP's authentication process "as conforming with the NIST guidelines for Authentication Assurance Level 2 (AAL2)." 91 Fed. Reg. at 25,228. The phrase "NIST guidelines" identifies neither a publication nor a revision. Because a requirement stated only as "NIST guidelines" cannot be assessed against a fixed text, the company requests that the regulatory text instead cite:

- **NIST SP 800-63-4**, *Digital Identity Guidelines*, as the governing suite;
- **NIST SP 800-63A-4** for the IAL2 identity-proofing requirements; and
- **NIST SP 800-63B-4** for the AAL2 authentication requirements.

This is consistent with ATF's own working premise: the preamble already cites the fourth revision by volume. *See* 91 Fed. Reg. at 25,219 n.23 (citing "NIST SP 800-63A-4 at 44").

The Proposed Rule contains no incorporation-by-reference statement, and the company does not assume one; what follows is conditional. If the final rule cites a NIST publication at a named revision and gives it legal effect, naming the publications by revision is the course the incorporation-by-reference framework contemplates, and nothing in that framework counsels against it. Where an agency gives incorporated material legal effect, 5 U.S.C. § 552(a)(1) provides that "matter reasonably available to the class of persons affected thereby is deemed published in the Federal Register when incorporated by reference therein with the approval of the Director of the Federal Register." The implementing regulations condition the Director's approval on the material being "reasonably available to and usable by the class of persons affected," 1

C.F.R. § 51.7(a)(3), and require the agency to "[d]iscuss, in the preamble of the final rule, the ways that the materials it incorporates by reference are reasonably available to interested parties and how interested parties can obtain the materials," *id.* § 51.5(b)(2).

Those conditions are readily satisfied here. NIST publishes SP 800-63-4 and its constituent volumes at no charge and without restriction, in full text, on a public website. A standard that any licensee, transferee, CSP, or assessor can obtain immediately and for free is the paradigm case of material "reasonably available to and usable by the class of persons affected." ATF's preamble discussion under § 51.5(b)(2) would accordingly be a brief one.

But naming the fourth revision without a transition would close the channel the Proposed Rule opens. The company raises this against its own preference, because it is the practical fact that decides whether this rule operates at all.

NIST SP 800-63-4 was published in **July 2025**. The Proposed Rule requires only that "[a]n independent third party must assess the CSP's remote identity proofing process as conforming with the National Institute of Standards and Technology (NIST) guidelines for Identity Assurance Level 2 (IAL2)." 91 Fed. Reg. at 25,228. It names no accreditor and requires no particular accreditation, and the company does not read it to require one; ATF mentions Kantara once, illustratively, in surveying who assesses conformance in the current market. *Id.* at 25,224. But the public accreditation register that assessor maintains is the best evidence available of what the market can presently supply, and it shows the difficulty plainly. As of the date of this comment, **not one credential service provider on that register holds a grant against the fourth revision.** Every provider currently holding an IAL2/AAL2 grant there is accredited against **revision 3**, including:

- **ID.me**, which the Proposed Rule's own preamble names as the IRS's example of IAL2 remote identity proofing — its grant reads "NIST 800-63 rev.3", in good standing to 2028;
- **CLEAR Verified** (Secure Identity, LLC), one of several full-service commercial providers at that level — the others accredited to both IAL2 and AAL2 in good standing include **athenahealth**, **Private Identity LLC** and **Exostar** — every one of them accredited against revision 3;
- **Login.gov**, the Federal Government's own service, accredited to revision 3 and in good standing to 2027.

The newest grant issued on that register in 2026 is also against revision 3. *(Verified against the Kantara Initiative Trust Status List, 2026-07-29.)*

So a final rule citing revision 4, effective on publication, would require licensees to use a class of provider that the market does not yet visibly supply — a class from which even the provider the preamble cites as the IRS's example is excluded. The requirement would not raise the bar; it would empty the room. A licensee cannot conjure a conforming provider, and a provider cannot obtain a fresh third-party assessment against a newly published revision on the day the rule takes effect — least of all in a certification market that ATF itself describes as controlled by "the very limited number of firms that currently dominate the market." 91 Fed. Reg. at 25,224.

The company therefore requests that the regulatory text cite the fourth revision, and add a transition:

> *Until credential service providers conformant with NIST SP 800-63-4 are available, a credential service provider conformant with NIST SP 800-63-3 at IAL2 and AAL2 satisfies this paragraph. The Attorney General shall publish notice when this sentence ceases to operate, effective not less than one year after publication.*

This preserves everything the precision request achieves — a fixed, citable, assessable text — while ensuring the rule can be complied with on the day it takes effect. It requires no waiver, no case-by-case determination, and no further rulemaking. **And it reaches the stronger standard by the only route that actually arrives there: as soon as the market can meet it.**

The company does not ask ATF to lower the standard. It asks ATF to adopt a standard that can be met, and to say when the higher one begins.

The framework further confirms that a fixed revision is the workable choice rather than an obstacle to one: incorporation "is limited to the edition of the publication that is approved," and "[f]uture amendments or revisions of the publication are not included." 1 C.F.R. § 51.1(f). It is the open-ended alternative — a citation drafted to absorb successor revisions automatically — that sits uneasily with that limitation, because it would give legal effect to text the Director has not approved and the public has not seen. A citation to a named publication at a named revision presents no such difficulty. Should ATF wish to track later revisions, it can do so through the ordinary course of a subsequent rulemaking, with notice and comment on the changed text.

The company accordingly requests that the final rule identify the specific publications and revisions on which § 478.96(c)(3)(ii) depends, and that it adopt the transition set out above.

B. Require the credential service provider to make phishing-resistant authentication available to the transferee

Proposed § 478.96(c)(3)(ii) requires the CSP's authentication process to conform to AAL2. NIST SP 800-63B-4 § 2.2.2 (Authenticator and Verifier Requirements), at 7, provides:

> "Verifiers SHALL offer at least one phishing-resistant authentication option at AAL2, as described in Sec. 3.2.5. Federal agencies SHALL require their staff, contractors, and partners to use phishing-resistant authentication to access federal information systems. In all cases, verifiers SHOULD encourage the use of phishing-resistant authentication at AAL2 whenever practical since phishing is a significant threat vector . . . ."

The publication's comparison of the authentication assurance levels is to the same effect: phishing resistance is "Not required" at AAL1, "Recommended; Must be available" at AAL2, and "Required" at AAL3. Availability is thus the AAL2 characteristic, and required use is reserved to AAL3. (Section 3.2.5, "Phishing Resistance," defines the term and the protocol property; it does not itself impose the requirement.)

The second sentence of the passage quoted above does not reach this transaction of its own force, and the company does not contend otherwise. On the Proposed Rule's facts the transferee authenticates to a private CSP, not to a federal information system; it is the licensee, not the transferee, who contacts NICS. NIST's own usage confirms the limit: the publication describes the federal enterprise scope as "those considered in scope for PIV guidance, such as government contractors, government employees, and

mission partners," and states that it "does not include government-to-consumer or public-facing use cases." NIST SP 800-63B-4, at 34 n.2. A NOTC transferee is a member of the public engaged in a consumer-facing transaction.

The company's request accordingly runs to the credential service provider and not to the transferee. The company requests that § 478.96(c)(3)(ii) state expressly that the CSP's authentication process must be capable of phishing-resistant authentication, as that term is described in NIST SP 800-63B-4 § 3.2.5, and must make at least one phishing-resistant option available to the transferee at no additional charge. **The company does not ask ATF to require a transferee to obtain, possess, or use any particular authentication technology, and does not ask that completion of a transfer be conditioned on the transferee's choice among the options a conformant CSP offers.** The requested provision would make the capability a condition of the CSP's eligibility, leaving the choice of authenticator where NIST leaves it at AAL2.

Three reasons support stating the requirement:

1. **It imposes no additional burden on CSP selection once the fourth revision governs.** Every verifier conformant with NIST SP 800-63B-4 must already offer at least one phishing-resistant option, so an express availability requirement does not narrow the field of eligible CSPs or require any CSP to build a new capability. That guarantee is a feature of the fourth revision, and the company does not represent that it holds under the third. The company therefore asks that this requirement take effect together with the fourth-revision citation, rather than during the transition period requested in Part II.A.
2. **It makes the capability assessable.** Proposed § 478.96(c)(3)(ii) turns on an independent third party's assessment of the CSP's authentication process. Stating the availability requirement in the regulatory text places it within the scope of that assessment, rather than leaving it to a general representation of conformance.
3. **The consequence of an authentication failure.** Identity proofing establishes who the transferee is on one occasion; authentication is what binds a later transaction to that proofed identity. If the transferee's credential is compromised, the NICS check required by § 922(t) is run against the identity of a person other than the one receiving the firearm. The check then does not do what the statute asks of it, and the lawful person whose identity was misused is left associated with a transaction that was not his or hers.

C. Limit the retention and use of transferee identity-proofing data

Proposed § 478.96(c)(3) directs the licensee to "ensure the transferee verifies their identity through a credential service provider (CSP) using a remote identity verification process." 91 Fed. Reg. at 25,228. Doing so places the information required to prove identity at IAL2 — name, date of birth, address, images of identity documents, and a live capture of the transferee's face — with a private party that is not a licensee, is not subject to the records provisions of Part 478, and whose handling of that information the Proposed Rule does not address. The facial capture is not conditional on how a given provider works. Proposed § 478.96(c)(3)(ii) provides that the CSP's "binding process must employ a live physical facial comparison by a CSP representative, or an automated biometrical facial comparison (e.g., 'selfie' verification), using a live capture of the transferee's facial image and liveness detection." *Id.* Both permitted pathways are facial comparisons, and the live capture and liveness detection required by the closing clause govern each of them. Every transferee who completes a NOTC transfer under this rule

therefore surrenders a live image of his or her face to a private credential service provider. The Proposed Rule states no limit on what the CSP may retain, for how long, or to what further use it may put what it collects.

The company requests that any final rule provide that identity-proofing and authentication data collected from a transferee under § 478.96(c)(3):

1. be used only for the verification that paragraph requires;
2. be retained no longer than necessary to complete that verification and any record the licensee is separately required to keep; and
3. not be aggregated, sold, licensed, disclosed for any other purpose, or used to compile or contribute to any list or record of persons who have acquired firearms.

The limitation follows the policy Congress set in 18 U.S.C. § 926(a), which provides that no rule or regulation prescribed after the enactment of the Firearms Owners' Protection Act "may require that records required to be maintained under this chapter or any portion of the contents of such records, be recorded at or transferred to a facility owned, managed, or controlled by the United States or any State or any political subdivision thereof, nor that any system of registration of firearms, firearms owners, or firearms transactions or dispositions be established." A rule that routes every remote transferee through a private credential service provider, while saying nothing about what that provider may keep or assemble, would permit the accumulation in private hands of precisely the record the statute forbids ATF to require — with the added feature that the accumulation would occur as a consequence of the federal rule rather than despite it. A private credential service provider should not become the vehicle for what § 926(a) denies to ATF directly.

The company accordingly requests that the limitation appear in the regulatory text as a condition of a CSP's eligibility under § 478.96(c)(3)(ii), so that it falls within the same independent third-party assessment on which that paragraph already relies.

D. Structured electronic format for chief law enforcement officer notice

The Proposed Rule "adds remote identity proofing and electronic notices to chief law enforcement officers." 91 Fed. Reg. at 25,216. The copy of the sworn statement and firearm description must be forwarded to the chief law enforcement officer "by registered or certified mail, or by electronic notification, in a form prescribed by the Attorney General." 91 Fed. Reg. at 25,217 (describing 18 U.S.C. § 922(c)(2), as amended by Pub. L. No. 118-159, div. E, tit. LII, § 5211(b), 138 Stat. 1773, 2449 (2024)).

The company requests that the form so prescribed be a structured, machine-readable format published by ATF, so that electronic notices can be ingested into law-enforcement record systems without manual re-entry and handled uniformly across jurisdictions.

III. Conclusion

Stone Bravo Outpost LLC supports finalization of the Proposed Rule with the modifications in Part II.

Respectfully submitted,

/s/ Warren Stone

Warren Stone
Founder, Stone Bravo Outpost LLC