Biometric Identity Verification RFP Checklist

Requirements, verification steps, scoring, demo tests, pilot criteria and contract clauses, in one checklist you can paste into an RFP or scoring workbook.

> **SHALL** mandatory: a missing item disqualifies the offer. **SHOULD** desirable: scored only. All attachments are due with the proposal.

BEFORE THE RFP

- [ ] Set the target assurance level yourself; do not let offerors choose it

ASSURANCE AND CERTIFICATION

- [ ] **SHALL** State the certified IAL, SP 800-63 revision and certifying body, and attach the listing URL and scope line
- [ ] **SHALL (if fingerprints in scope)** Name each fingerprint capture device by model and attach its FBI CPL entry
- [ ] **SHOULD** Provide a date for SP 800-63 revision 4 assessment and attach a signed schedule

CAPTURE AND ATTACK RESISTANCE

- [ ] **SHALL (remote collection) / SHOULD (attended)** Provide an ISO/IEC 30107-3 report per modality from an accredited lab
- [ ] **SHALL** Describe the injection attack defense and attach the technical description
- [ ] **SHOULD** Provide independent injection test results (e.g. CEN/TS 18099)
- [ ] **SHALL** Name the matching algorithm for each modality
- [ ] **SHOULD** Provide independent matcher results (e.g. NIST FRTE/IREX), including demographics where applicable
- [ ] **SHALL (if passports in scope)** Read the MRZ and RFID chip and validate the chip's certificates
- [ ] **SHALL (if PIV cards in scope)** Read the chip and validate its certificates

SUPERVISION AND EVIDENCE

- [ ] **SHALL (IAL3/PIV) / SHOULD (IAL2)** Describe the operator role, training and override rights
- [ ] **SHALL** Produce an exportable, tamper-evident session record and attach a redacted sample
- [ ] **SHOULD** Support supervised remote operation per FIPS 201-3 Sec. 2.7.1
- [ ] **SHOULD** Offer an alternate path at the same assurance level

DATA HANDLING

- [ ] **SHALL** Provide a policy on stored data, retention, encryption, key custody and data location
- [ ] **SHALL** State whether customer data trains models, and list sub-processors with locations
- [ ] **SHOULD** Delete data on request and prove the deletion

IMPLEMENTATION AND INTEGRATION

- [ ] **SHALL** Offer documented interfaces to IDMS, PACS and HR systems, including credential binding
- [ ] **SHALL** Provide expected failure-to-enroll, abandonment and throughput rates, with the basis for each
- [ ] **SHOULD** Provide an implementation plan with timeline, staffing and responsibilities

FEDERAL ADD-ONS

- [ ] **SHALL (if applicable)** Provide GSA FIPS 201 APL status for PIV cards and readers in scope
- [ ] **SHALL (if applicable)** Provide FedRAMP authorization or the ATO path for cloud components
- [ ] **SHALL (if applicable)** Describe the fingerprint submission path for background investigations
- [ ] **SHALL (if applicable)** Provide Section 508 conformance documentation
- [ ] **SHALL (if applicable)** Provide the support needed for your Privacy Act SORN and PIA

VERIFY YOURSELF

- [ ] Look up the Kantara TSL entry and record level, revision, service type and scope line
- [ ] Check the 30107-3 report for lab accreditation, modality, attack types and IAPAR
- [ ] Search the FBI CPL by exact model; treat it as proof of image quality only
- [ ] Confirm the NIST FRTE/IREX version matches and read the demographic results
- [ ] Treat red-flag answers as missing evidence

SCORING

- [ ] Disqualify any offer missing a SHALL item or attachment (Stage 1)
- [ ] Score each row 2 / 1 / 0, divide by 2, multiply by the weight, total out of 100 (Stage 2)
- [ ] Write cell definitions before proposals arrive
- [ ] Evaluate price separately

LIVE DEMO

- [ ] Attempt a virtual camera or replayed stream injection
- [ ] Read a passport and/or PIV card chip and show certificate validation
- [ ] Run a real exception and confirm the decision and any override are logged
- [ ] Export the session record on the spot

PILOT

Set pass lines before the first applicant.

- [ ] Measure failure-to-enroll rate (any path / started; alternate paths at target level)
- [ ] Measure throughput in the defined peak window
- [ ] Measure abandonment rate and log a reason for each case
- [ ] Collect a complete assessor evidence package

CONTRACT

- [ ] Commit to a revision 4 assessment date
- [ ] Give notice if a listing lapses or its scope changes
- [ ] Set SLAs for uptime and support response, with credits
- [ ] List the pricing model, all fees and total cost
- [ ] State model training terms
- [ ] Define the exit plan and data return
- [ ] Certify deletion after data return
- [ ] Give breach notice within the agreed window
- [ ] Name sub-processors and data locations, with notice of change

How to use each item, the scoring rubric and the red-flag answers: nextgenid.com/biometric-identity-verification/rfp-checklist/