

APPENDIX F

Security & Data Privacy Certification Form

AFI Translation Services — Request for Proposals

Purpose

This certification form must be completed and submitted by all Offerors responding to the AFI Translation Services RFP. It serves to verify that the Offeror's practices, systems, and policies comply with applicable data security standards, data residency requirements, and restrictions on the use of agency data — including the prohibition on using agency-provided content for AI model training without explicit written consent.

Submission of this form constitutes a binding certification. Misrepresentation or material omission may result in disqualification, contract termination, and/or other remedies available under applicable law.

Part I — Offeror Identification

Legal Name of Offeror:	Bluejay AI Technologies Inc.
DBA / Trade Name (if applicable):	N/A
Primary Business Address:	4200 Cheeney Street, Santa Clara, CA 95054
DUNS / UEI Number:	DUNS: 119162986 / UEI: KTEPUMM1APA1
Name of Authorized Certifying Official:	Joseph Barrientos Liba
Title:	Chief Executive Officer / Chief Technology Officer
Email Address:	support@bluejayai.net
Phone Number:	(978) 799-7069
Date of Submission:	May 11, 2026

Part II — Security & Data Privacy Certification Checklist

For each requirement below, indicate compliance status and provide any relevant notes or explanations.

#	Requirement	Compliance Status	Notes / Explanation
A. Data Security Standards			
A1	Offeror maintains and operates under a documented Information Security Program (ISP) aligned with a recognized framework (e.g., NIST SP 800-53, ISO 27001, SOC 2 Type II).	☒ Yes ☐ No ☐ N/A	SOC 2 Type II certified by InterCert (Q1 2025). NIST SP 800-53 aligned Information Security Program in place.
A2	All data in transit is encrypted using TLS 1.2 or higher. All data at rest is encrypted using AES-256 or equivalent standard.	☒ Yes ☐ No ☐ N/A	TLS 1.3 in transit; AES-256 at rest across all AWS storage layers.

A3	Offeror conducts regular vulnerability assessments and penetration testing (at least annually) on systems used to process agency data.	☒ Yes ☐ No ☐ N/A	Annual third-party penetration test conducted in conjunction with SOC 2 audit (most recent Q1 2025). Next scheduled Q3 2026.
A4	Offeror maintains a documented incident response plan and will notify the agency within 72 hours of any confirmed data breach or security incident involving agency data.	☒ Yes ☐ No ☐ N/A	Documented incident response plan in place. Agency notification within 72 hours of confirmed breach — contractually committed.
A5	Access to agency data is restricted to authorized personnel only, governed by role-based access controls (RBAC) and the principle of least privilege.	☒ Yes ☐ No ☐ N/A	Role-based access controls (RBAC) enforced. Principle of least privilege applied to all internal systems and cloud infrastructure.
A6	Multi-factor authentication (MFA) is enforced for all personnel accessing systems that process or store agency-provided content.	☒ Yes ☐ No ☐ N/A	MFA enforced via authenticator app (TOTP) for all personnel accessing production systems, cloud console, and agency data environments.
A7	Offeror maintains audit logs of all access to and handling of agency data, retained for a minimum of 12 months.	☒ Yes ☐ No ☐ N/A	Audit logs retained in AWS CloudWatch with 12-month retention policy. Access logs available for agency review upon request.
B. Data Residency & Sovereignty			
B1	All agency-provided data will be stored, processed, and transmitted exclusively within the United States, unless an alternative jurisdiction has been expressly approved in writing by the agency.	☒ Yes ☐ No ☐ N/A	All agency data stored and processed exclusively in AWS us-east-1 (N. Virginia) and us-west-2 (Oregon). No offshore processing.
B2	Offeror will not transfer, replicate, or back up agency data to servers, cloud regions, or subcontractors located outside the approved jurisdiction without prior written agency authorization.	☒ Yes ☐ No ☐ N/A	No cross-border data transfer. Backup replication occurs only between approved US regions.

B3	Offeror can identify and document the specific data centers and/or cloud regions used to process and store agency content upon request.	☒ Yes ☐ No ☐ N/A	AWS us-east-1 and us-west-2. Specific data center documentation available upon request.
B4	Subcontractors and third-party vendors used in the delivery of translation services are bound by data residency obligations no less restrictive than those in this certification.	☒ Yes ☐ No ☐ N/A	All subcontractors and third-party vendors (including Soniox and translation API providers) operate under DPAs with equivalent or stricter data residency requirements.
C. AI & Machine Translation — Prohibition on Unauthorized Training			
C1	Offeror will NOT use agency-provided documents, content, translations, glossaries, terminology databases, or any derivative thereof to train, fine-tune, update, or improve any AI or machine learning model without the agency's explicit prior written consent.	☒ Yes ☐ No ☐ N/A	Agency-provided content is never used to train, fine-tune, or improve any AI or ML model. Zero-retention policy enforced with all third-party providers.
C2	If machine translation (MT) engines or large language models (LLMs) are used in the workflow, Offeror confirms that agency data is processed in a data-isolated environment and is not retained by the MT/LLM provider beyond the scope of the individual translation task.	☒ Yes ☐ No ☐ N/A	All agency content processed in stateless, isolated API calls. No content is retained by Soniox or other providers beyond the individual request.
C3	Offeror discloses the use of any third-party MT engines, AI translation tools, or LLM APIs (including the provider name and model) in the space provided on this form.	☒ Yes ☐ No ☐ N/A	ASR Engine: Soniox (speech recognition). Translation Engine: Google Gemini (translation/generative AI). Both operate under zero-retention DPAs.
C4	Offeror has contractual agreements with any MT/LLM third-party providers explicitly prohibiting those providers from using agency data for model training, product improvement, or any purpose beyond task execution.	☒ Yes ☐ No ☐ N/A	Data Processing Agreements (DPAs) in place with all ML/AI providers explicitly prohibiting use of customer content for training, fine-tuning, or product improvement.
C5	Offeror will promptly notify the agency if any MT/LLM provider changes its data usage terms in a manner that could affect compliance with this certification.	☒ Yes ☐ No ☐ N/A	Bluejay monitors provider terms of service and will notify the agency within 5

			business days of any material change affecting data usage compliance.
C6	Upon contract expiration or termination, Offeror and all sub-processors will securely delete or return all agency-provided data within 30 days and provide written certification of deletion.	☒ Yes ☐ No ☐ N/A	All agency-provided data and derivatives securely deleted within 30 days of contract expiration or termination. Written deletion certification provided.
D. Personnel & Subcontractor Obligations			
D1	All personnel (including subcontractors) with access to agency data are bound by written confidentiality agreements and have received data privacy and security training within the past 12 months.	☒ Yes ☐ No ☐ N/A	All personnel with data access are bound by signed NDAs and have completed security awareness training. Annual training cycle; next Q3 2026.
D2	Offeror has conducted background checks on all personnel who will have access to sensitive or controlled agency content, consistent with applicable laws and regulations.	☒ Yes ☐ No ☐ N/A	Comprehensive background checks (identity and criminal) are conducted on all personnel with production access prior to employment.
D3	Offeror will not reassign primary translation personnel to tasks involving agency data without prior notification to the agency's Contracting Officer's Representative (COR).	☒ Yes ☐ No ☐ N/A	Confirmed. Strict role-based access controls ensure personnel are not reassigned to agency tasks without prior authorization.
E. Compliance, Certifications & Regulatory Alignment			
E1	Offeror is compliant with all applicable federal and state data privacy laws, including but not limited to FISMA, Privacy Act of 1974, and any agency-specific data handling requirements communicated in the RFP.	☒ Yes ☐ No ☐ N/A	Fully compliant with applicable federal and state data privacy laws, including the Privacy Act of 1974.
E2	If handling any Controlled Unclassified Information (CUI), Offeror is or will be compliant with NIST SP 800-171 and any applicable CMMC level requirements.	☐ Yes ☐ No ☒ N/A	Bluejay AI does not currently process CUI. If CUI processing is requested by a specific agency, we will align with NIST SP 800-171 prior to task execution.
E3	Offeror holds or will obtain the following third-party security certifications (check all that apply): SOC 2 Type II / ISO 27001 / FedRAMP Authorization / Other (describe in notes).	☒ Yes ☐ No ☐ N/A	SOC 2 Type II certified (InterCert). ISO 27001 in process

			(targeting Q4 2026). FedRAMP Tailored roadmap for 2027.
E4	Offeror will provide the agency with updated copies of relevant compliance certifications or audit reports upon request and upon renewal/expiration.	☒ Yes ☐ No ☐ N/A	Confirmed. All audit reports and compliance certifications are available to participating agencies under NDA.

Part III — Machine Translation & AI Tool Disclosure

Offerors using any AI-assisted translation tools, machine translation engines, or large language model APIs must complete this section. If no AI or MT tools are used, indicate below and skip to Part IV.

☐ No AI or machine translation tools are used in our workflow. All translation is performed by human translators only.

Tool / Platform Name	Provider / Vendor	Role in Workflow	Data Retained by Provider?
Soniox API	Soniox Inc.	ASR / Speech-to-Text & Diarization	No (Zero-retention DPA)
Gemini 2.0 Flash	Google Cloud	Primary Translation Engine	No (Zero-retention Enterprise API)
OpenAI TTS / GPT-4o	OpenAI	Audio Synthesis / Fallback Engine	No (Zero-retention API policy)
ElevenLabs API	ElevenLabs	Dubbing / Voice-over synthesis	No (Enterprise privacy tier)
Azure AI Document	Microsoft	OCR for scanned documents	No (FedRAMP compliant)

Attach copies of relevant data processing agreements (DPAs) or terms with each MT/AI provider as a sub-exhibit to this Appendix. Standard Enterprise DPAs enforcing zero-retention are on file and available for AFI review upon request.

Part IV — Exceptions & Deviations

If the Offeror cannot fully comply with any requirement listed in Part II, identify each item by number, state the nature of the limitation, and propose an equivalent alternative safeguard below. The agency reserves the right to determine whether any proposed alternative is acceptable.

Item #	Nature of Non-Compliance or Limitation	Proposed Alternative Safeguard	Estimated Compliance Date

Part V — Certification & Authorized Signature

Certification Statement

- I, the undersigned authorized representative of the Offeror, hereby certify that:
- The information provided in this certification form is true, accurate, and complete to the best of my knowledge.
 - The Offeror has implemented, or commits to implementing prior to contract award, all applicable security and data privacy controls described herein.
 - Agency-provided data will not be used to train, fine-tune, or improve any AI or machine learning model without prior explicit written consent from the agency.
 - The Offeror understands that knowingly providing false information may result in disqualification, contract termination, suspension or debarment, and/or referral for legal action.

Signature of Authorized Official *Joseph Barrientos Liba*
Date: May 11, 2026

Joseph Liba
Printed Name

CEO

Bluejay AI Technologies Inc
Organization Name

Submission Instructions

This completed and signed form, along with any required attachments (DPAs, compliance certifications, sub-exhibit disclosures), must be included as Appendix F in the Offeror's proposal submission. Electronic signatures are acceptable. Unsigned or incomplete forms may result in disqualification.