

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:	Global Interpreting Network Inc.
DBA / Trade Name (if applicable):	
Primary Business Address:	25060 Avenue Stanford, Suite 155 Valencia, CA 91355
DUNS / UEI Number:	826315512 / RVWNWMDX2KL3
Name of Authorized Certifying Official:	Joe Whittington
Title:	VP Sales
Email Address:	jwhittington@globalinterpreting.com
Phone Number:	Direct: 602-877-5537
Date of Submission:	May 8, 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	
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	

A3	Offeror conducts regular vulnerability assessments and penetration testing (at least annually) on systems used to process agency data.	☒ Yes ☐ No ☐ N/A	
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	
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	
A6	Multi-factor authentication (MFA) is enforced for all personnel accessing systems that process or store agency-provided content.	☒ Yes ☐ No ☐ N/A	
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	
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	
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	
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	
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	
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	
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	
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	
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	

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	
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	
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	
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	
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	
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	
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	
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	
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	

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?
AI/MT Engine	AWS Translate DeepL Google NMT Azure Translator	- AWS Translate: WS1/WS3 Translation - DeepL/GoogleNMT/Azure Translator: WS2 Translation	- AWS Translate: No model training (Via Opt-out policies)

			- Azure Translator: Data, privacy, and security for Azure Translation in Foundry Tools. No persistent storage by design across all API tiers. - DeepL: Terms and Conditions. Temporarily stored only as technically required for service delivery. In exceptional debugging cases, up to 72 hours encrypted, then auto-deleted. No persistent storage by default. Not used for AI model training. - Google NMT (Cloud Translation): Data usage FAQ. Text held in-memory only during translation; no persistent storage. - Azure Translator: Data, privacy, and security for Azure Translation in Foundry Tools. No persistent storage by design across all API tiers.
LLM(s) Used	OpenAI GPT-4o/GPT-4o-mini	- OpenAI: WS1/WS3 Contextualization Layer	OpenAI: Data Controls in the OpenAI Platform. 30 day retention for abuse monitoring, then deleted.
Translation Approach	- NMT (AWS Translate, DeepL, Google NMT, Microsoft Translator) - Generative AI (OpenAI)	Translations	None
Third-Party Services	- Soniox - Azure TTS	- Soniox: WS1/WS3 ASR - Azure: WS1/WS3 TTS	- Soniox: Soniox Privacy Policy). Audio and transcript data not stored by default and not used for model training. - Azure TTS: Microsoft Azure Cognitive Services Data Privacy Documentation. Real-time processing only, no persistent storage.

Attach copies of relevant data processing agreements (DPAs) or terms with each MT/AI provider as a sub-exhibit to this Appendix.

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.

N/A

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.

Joe Whittington

Signature of Authorized Official

May 8, 2026

Date

Joe Whittington

Printed Name

VP Sales

Title

Global Interpreting Network 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.