

ARTIFICIAL INTELLIGENCE (AI) QUESTIONNAIRE

Preliminary Screening

	Item	Question	Vendor Response
<input type="checkbox"/>	1	Do you test your models for security, privacy, and vulnerabilities?	
<input type="checkbox"/>	2	Is our data used to improve any AI/ML model?	
<input type="checkbox"/>	3	Do any third parties receive or process our data?	
<input type="checkbox"/>	4	Can we opt out of training and data retention?	
<input type="checkbox"/>	5	If not using AI/ML now, do you have any plans to use it in the future?	
<input type="checkbox"/>	6	Can AI inputs, outputs, and decision logic be logged, retained, and produced to support audits, investigations, or Public Records Requests? And are outputs explainable to non-technical stakeholders?	
<input type="checkbox"/>	7	Which standards or frameworks do you align with (NIST AI RMF)?	
<input type="checkbox"/>	8	Do you address OWASP Top 10 for your AI Category (https://owasp.org/www-project-top-10-for-large-language-model-applications/)? If so, how?	
<input type="checkbox"/>	9	Where will the AI solution be located?	
<input type="checkbox"/>	10	How is the model trained?	
<input type="checkbox"/>	11	What inputs does the model require?	
<input type="checkbox"/>	12	Does the vendor have ai solution data flows and a diagram showing flow of traffic through encoders/decoders etc?	
<input type="checkbox"/>	13	What does the model output?	
<input type="checkbox"/>	14	Who owns any/all output(s)?	