

**Partner Onboarding**

**USAi**

# Agenda

**01.**

USAi demo

**02.**

Partner onboarding  
details

**03.**

Next steps &  
questions

# Demo



# USAi platform



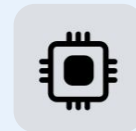
## Chat

A chatbot interface with multiple foundational, premier models



## Console

Analytics dashboard for usage, safety, and model evaluations



## API

Application Programming Interface to integrate AI into your workflow

# Partner onboarding

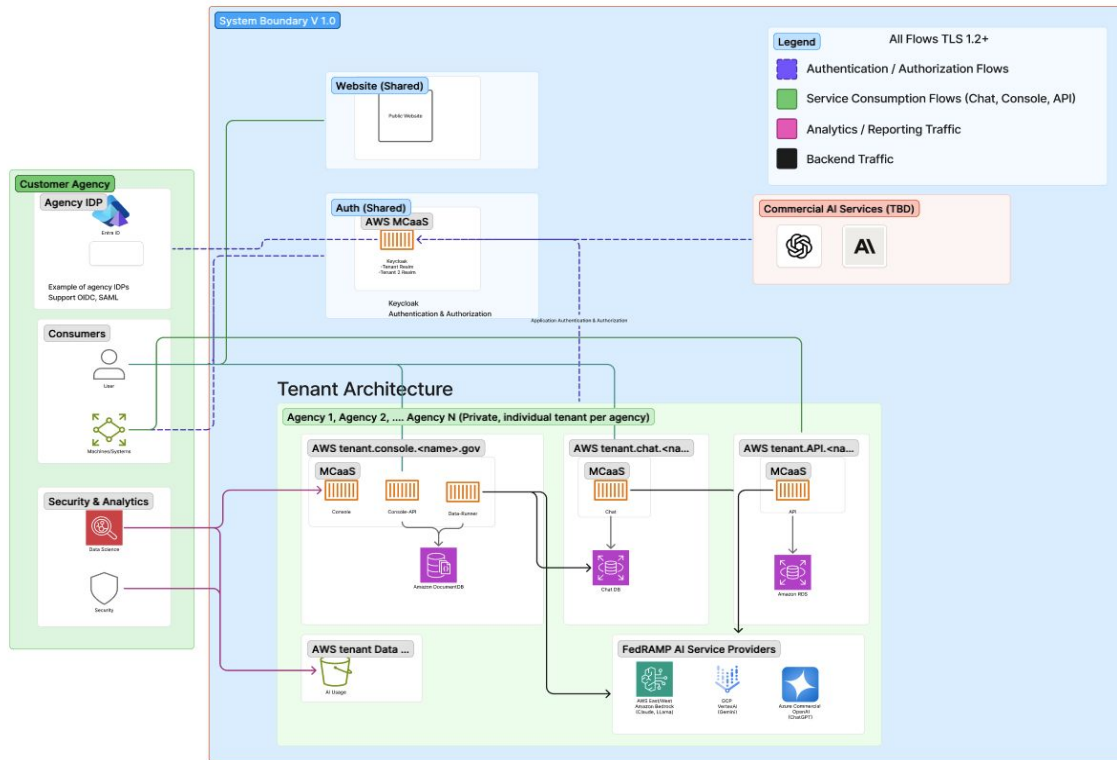


# Shared responsibility model



# 🔒 Secure: Federated architecture

- Tenant isolation
- Single-sign on
- Audit logging
- Faster ATO reuse
- Universal model access via FedRAMP-authorized hyperscalers
- Continual expansion of available commercial service access
- Flexible architecture to support diverse agency mission requirements



# USAi Partner Log Availability



## Security Logs

- Retained 180 days within the platform; further maintained in GSA SOC
- Can be made available to Agency SIEM on request



## Raw Prompt & Response

- Users' raw interactions with AI (+ tags/metadata)
- Stored in RAW S3 for 30 days; agency must ingest into their system for analysis/retention
- Not used by USAi for internal analytics



## Redacted Prompt & Response

- User specific identifiers and sensitive PII data removed
- Used for console metrics dashboards & customer log downloads
- Stored in Redacted S3



## Compliant: Built for government

- **Secure:** USAi utilizes FedRAMP moderate or high authorized services to deliver its chat, API, and console services.
- **Continuously monitored:** GSA ensures our solution as well as the services we use are continuously monitored, allowing agencies to focus on their AI needs.
- **Vetted and tested:** Standardized safety/performance evaluations, system-prompt transparency, and support for agency AI inventory/assessments.

## Compliant: Data protection and privacy

- **Dedicated workspaces:** USAi provides each partner agency with its own dedicated tenant workspace.
- **Agency-control over data:** Agencies retain full control over its data.
- **Protecting sensitive information:** USAi uses automated systems to redact sensitive information and to generate metrics and other insights. The agency governs CUI/PII use per policy.

# Transparent: Data protection and privacy

## USAi collects:

GSA + agency receive	Agency receives
<b>User contact and organization information</b> <ul style="list-style-type: none"><li>• Your user's name, email address, organization information, and when your users access the service to authenticate into it.</li></ul>	<b>Interaction information</b> <ul style="list-style-type: none"><li>• Prompts and responses, uploaded documents, searches, feedback information (thumbs-up / thumbs-down), connection information, and usage information.</li></ul>

## 🔒 Secure: Prompt & response logging

- **User Conversations:** Users manage their own conversations. USAi and Agencies are not provided access to saved conversations.
- **Raw interactions (30 days):** Agencies can access raw prompts & responses from chat and API for 30 days.
- **De-identified analytics:** Agencies and USAi use redacted, de-identified prompts/responses to power dashboards and analytics.
- **Separate from security logs:** Security/audit logging (e.g., authentication, admin actions) is distinct and does not include chat or API content

## Trustworthy: Vetted and tested AI solutions



- Access to multiple American AI models across the industry in a central platform.
- Vetted AI models and services that align with federal mandates such as Executive Orders, OMB memos, and other regulations.
- USAi provides out of the box performance, bias, and safety evaluations to help your users select the most trustworthy and cost-effective model for their needs, and prevent unbiased, fair, and non-harmful responses.
- Ongoing monitoring, versioning/notifications, and reciprocity with industry benchmarks.

# Model review process



## Procurement and onboarding

Ensure AI services meet GSA security, compliance, and operational standards



## Implementation & testing

Establish performance baselines, ensure consistent service quality and that models are unbiased and appropriate



## Operations and monitoring

Detect and respond to model performance changes, safety issues, and (monthly/on-change) evaluations for performance, safety, and bias



## Governance and improvement

Easy access to model cards, system prompts, and ongoing feedback opportunities to improve USAi to meet your needs.

# Shared responsibility model

	USAi responsibilities	Partner responsibilities
<b>Service</b>	<ul style="list-style-type: none"><li>• Maintain platform access and continually onboard new models</li><li>• 25K token allowance</li></ul>	<ul style="list-style-type: none"><li>• Manage usage and costs</li></ul>
<b>Security</b>	<ul style="list-style-type: none"><li>• Security and maintenance of core infrastructure</li><li>• Gain general ATO</li></ul>	<ul style="list-style-type: none"><li>• Track implementation of security measures</li><li>• Designate POCs</li><li>• Leverage GSA ATO for agency authentication</li></ul>
<b>Implementation</b>	<ul style="list-style-type: none"><li>• Support integration</li></ul>	<ul style="list-style-type: none"><li>• Ensure usage compliance</li></ul>
<b>Operations</b>	<ul style="list-style-type: none"><li>• Provide monitoring tools</li><li>• Technical guidance</li></ul>	<ul style="list-style-type: none"><li>• Test and compare models</li><li>• Ensure compliance</li><li>• Train and manage users</li></ul>
<b>Support</b>	<ul style="list-style-type: none"><li>• Help desk support</li><li>• Provide feedback mechanism</li></ul>	<ul style="list-style-type: none"><li>• Tier 2 help desk for agency-specific usage</li></ul>
<b>Data</b>	<ul style="list-style-type: none"><li>• Redaction data pipeline and metrics</li></ul>	<ul style="list-style-type: none"><li>• Own and manage user data and usage</li></ul>

# Security operations



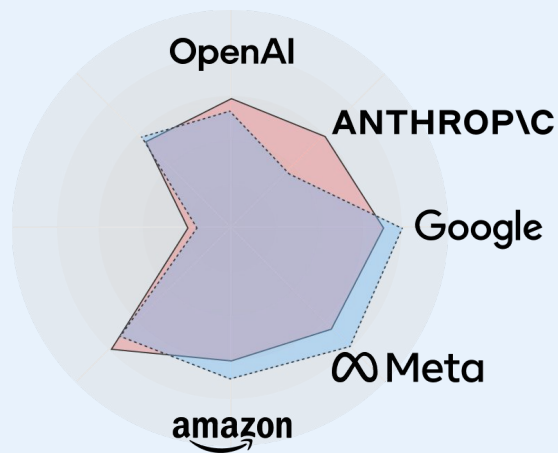
**USAi provides** secure infrastructure

## Partner agency will:

- Identify and manage user accounts.
- Work with USAi to implement and test authentication and authorization.
- Designate Performance, Security, and Privacy POC to provide feedback on service performance, security, and privacy.
- Track the implementation of security measures within the USAi service as well as agency integration with the USAi service.



# Model evaluation

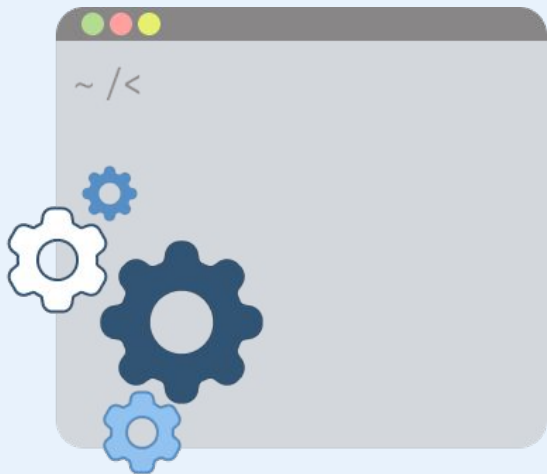


**USAi provides** baseline performance and bias testing to ensure the overall safety of models

## Partner agency will:

- Experiment and test with different AI models.
- Evaluate model performance based on agency use cases.
- Select best performing model for user needs.
- Launch vetted models only into production.

# Model adjustments and tuning



**USAi provides**  
recommended, tested  
system prompts

## Partner agency will

- Create and maintain their own agency-specific system prompts.
- Evaluate use cases after making changes to the prompt for safety and performance.
- Document modifications and monitor outputs.
- ⚠ Remember: You own your system prompt configuration and its outcomes.

# User training



**USAi provides** model cards, user guides, and reports.

## Partner agency will:

- Provide agency-specific guidance on privacy, and data types that are allowed.
- Manage agency AI use case process and governance.
- Conduct instructor-led training (optional).

# Monitoring usage and costs



**USAi provides** no-cost trial of up to \$25,000 of total token spend during the 6 month trial

## Partner agency will:

- Document all AI use in your agency's AI Inventory.
- Closely monitor uses that are high-impact.

 **Tip:** Compare model costs - some models are 10x more expensive per token.

# What happens next

We are here



1

## Kick-off call

USAi and partner agency meet to align on goals, timeline, and tee up key decisions.

2

## System training

USAi will provide system prompt training and empower partner agencies to manage their instance.

3

## Ongoing meetings

USAi and partner agency will hold recurring meetings to discuss findings, challenges, and needs.

4

## Project closeout

If decision is made to not renew, data and tenant instance will be destroyed, and we'll work with you to evaluate trial effectiveness.

# Next steps

## Checklist

- ☐ Work with us to integrate to your single sign-on solution.
- ☐ Identify admins who will have access to the raw logs (interaction, security logs).
- ☐ Identify if/how you'd like to retrieve log data every 30 days (interaction, security logs).
- ☐ Determine your AI use case and/or privacy policy (e.g. CUI, PII).
- ☐ Review our security package.
- ☐ Modify system prompts as appropriate.
- ☐ Determine models to deploy.
- ☐ Determine whether you would like document upload and/or web search enabled on Chat.
- ☐ Determine API user management flow.

**Thank you!**

# Appendix




# Commercial services access and usage



**USAi provides** access to certain commercial services

## Partner agency will:

- Authorize your use of the service
- Train users on service-specific features and limitations
- Ensure compliance with your agency's policies on each service
- Manage any service-specific workspace settings
- Monitor usage across multiple platforms

 Note: Commercial services may have different capabilities than USAi Chat

**COMING  
SOON**