Government AI Coalition

January 25, 2024

Albert Gehami (Albert.Gehami@sanjoseca.gov)

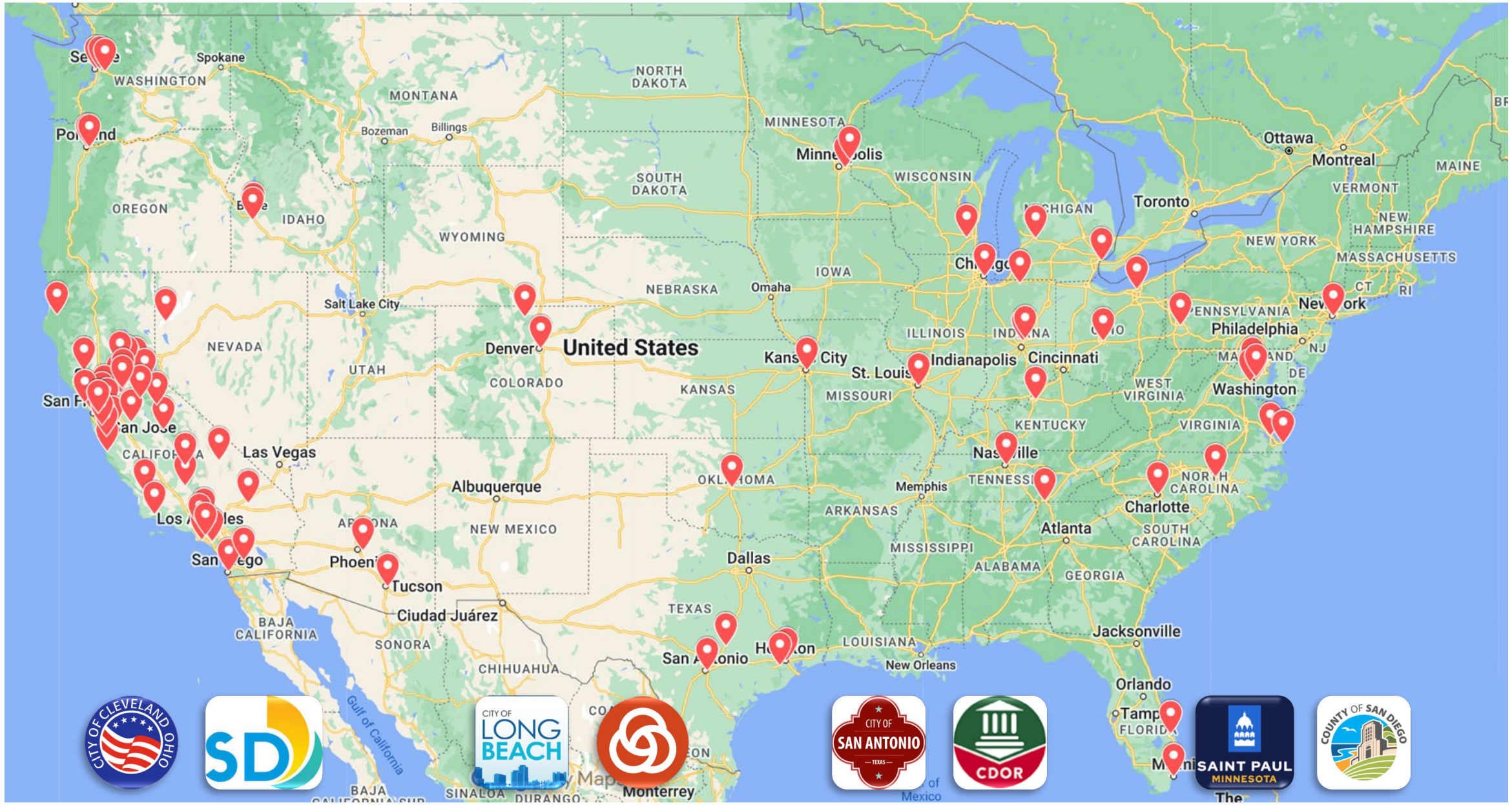
Leila Doty (Leila.Doty@sanjoseca.gov)

Matthew Jacquez (Matthew.Jacquez@sanjoseca.gov)

Agenda

1. Welcome – new folks introduce yourself in the chat!
2. Coalition Updates:
   - US Conference of Mayors
   - Context for newcomers
3. AI FactSheet
4. Working Group Updates
5. Open Letter
6. Next steps

Coalition: 140 agencies, 280 users



Coalition update: Conference of Mayors

Roadmap

Phases

- Phase I – Establish (4 months)
- Phase II – Expand (~12 months)
- Phase III – Maintain

Phase I

- Government agencies only
- Consensus on AI FactSheet
- "**One-stop-shop**" for all documents needed to set up your AI governance

Phase II

- Support implementation
- Launch Vendor Registry
- Build out use cases
- Explore new opportunities for partnership (e.g., data sharing)

GovAI Coalition, how does it all fit?

Tools to go from 0 to 90 in using AI in Government

1. How do I prepare my agency to use and govern AI?

Policy WG
Principles, Policy, and Processes

2. What can I do with AI that adds value?

Use Case WG
Starter guides & shared resources

3. Who can I work with for good, responsible AI solutions?

Vendor Registry WG
Database of vendor factsheets + other details

4. How do I ensure vendors follow my expectations?

Vendor Agreement WG
Standards and Requirements for AI Systems (legal addendum)

5. How do I prepare for when things go wrong?

Incident Response WG
AI Incident Response Plan

AI Factsheet (Coalition-wide)
Nutrition facts of the AI

GovAI – What's next for Phase 2?

Policy

Policy Committee: Monitor updates to AI policies; organize updates to templates; manage collaboration with federal government

Vendor relations

Vendor Registry committee: Maintain registry on teams, then oversee the platform development

Application

Implementation committee: "Office hours" for policy implementation support and applying use cases

New (start time varies)

Cooperative purchasing

Designing shared data architecture

Funding Committee – identifies and applies for joint grants (e.g., conference, registry platform, dedicated resource)

Standardized AI FactSheet

The “Nutrition Facts” of an AI system

Value: Informs purchasing, guides usage, and directs industry

Goal: Vote on Public “Version 1”

AI FactSheet for Third Party Systems

Please provide details regarding your Artificial Intelligence (AI) product by filling out the FactSheet[1] template below. You can find an example of a completed FactSheet on page 3.

FactSheet

Vendor Name	
System Name	
Overview	Brief summary of the AI system.
Purpose	What function does the AI system perform, and for what purpose?
Intended Domain	What domain is the AI system intended to be applied in?
Training Data	How was the AI system trained? What data was used? How often is data added to the training set?
Test Data	What data was used to test system performance? Under what conditions has the system been tested?
Model Information	General description of the model(s) used (e.g., large language model, transformer, deep learning, supervised learning, built on an existing open source model, computer vision)
Update procedure	In general, how often are the models updated for users? Will the user have a choice in moving to the updated model or staying on the current model?
Inputs and Outputs	What are the inputs to the AI system? What are its outputs?

Working Group Updates

Goal: Share draft deliverables and gather feedback for 4 of 5 working groups

Policy working group to share offline

Next Meeting: Discuss and vote on deliverables

Feedback form: http://bit.ly/GovAI-feedback

Use Case Working Group Update:

Use Case Template

Chairs:
- *Jaime Wascalus (St. Paul, MN)*
- *Jiri Rutner (San Diego County, CA)*
- *Omar Naseef (Austin, TX)*

Template Overview:

This document serves as a template for others to create their own tailored use cases. It is meant to illustrate a strategic method for using AI technology in solving challenges in state and local governments.

All sections do not need to be completed when first filling this out. Sections can start as considerations (or blanks), and more information can be added in depth as the use case is continued.

Examples can be found in the AI Use Cases Working Group folder.

Proposed Use Case:

In a sentence, what is your use case? What is the question you are trying to answer or problem to solve?

Proposed AI:

What kind of AI tool is being used and how is it being used? Is it a conversational chatbot or language model? Does the AI use computer vision or audio identification? Is the AI meant for prediction or for studying causal impact?

Proposed Project Phases:

Consider what phases your project might have. Can start with your proposed phases, and update as you progress in your use case. Potential phases could include:

1. **Pilot Program Development:** Assess readiness and explore feasibility.
2. **Training Phase:** Focus on understanding AI training techniques and methodologies.
3. **Capacity Building:** Assemble a skilled team for project development and conduct initial assessments.
4. **Testing and Validation:** Gather data on the performance of the system in the field. Once complete, add that performance report here for other agencies to learn.

Potential Benefits:

When possible, try to quantify the benefits, like cost savings or added value. Even if we can't assign a number, showing that there are quantifiable benefits can often help.

System and Project Challenges:

What kind of challenges do you anticipate in implementation? Can be very general in the planning phase as just considerations. As you implement your use case, add the major hurdles you experienced.

People/Domains to Involve:

Who or what groups need to be involved in this project? Where possible, consider when they should be involved as well. Some general groups to consider:

TEMPLATE

Use Case WG Deliverable: Framework for sharing use cases

Purpose

1. Provide agencies a guide for valuable AI use cases that can be shared in a standardized way
2. Templatize the pitch, resources, and considerations for use cases
3. Update each other on what works and what doesn't for specific use cases

What does the template cover?

1. Template Overview
2. Proposed Use Case
3. Proposed AI
4. Proposed Project Phases
5. Potential Benefits
6. System and Project Challenges
7. People/Domains to involve
8. Risks & Mitigation Strategies
9. Project Resources Needed
10. Data Sources
11. Combatting AI Bias

AI Incident Response Working Group Update:

AI Incident Response Plan Template

Chair: Jonathan Behnke (San Diego, CA)

AI Incident Response

Introduction

The AI Incident Response Plan (IRP) serves as the first line of defense for the [Agency Name] in case of an AI incident. This incident response document has been created based on the NIST AI Risk Management Framework and the Special Publication 800-61 Computer Security Incident Handling Guide.

Incident response occurs in sequential phases, each one building upon the next. The following phases provide a foundation for an Incident Response (IR) team to respond to and recover from an AI incident: Preparation, Identification, Containment, Eradication, Recovery, Lessons Learned.

Purpose

The purpose of this document is to prepare and gain fundamental understanding of the processes involved, the responsibilities, and the actions required to mitigate an AI incident. It is critical to identify and resolve incidents quickly before they escalate into a major incident with the potential to cause harm or damage to people, data, or the [Agency].

Scope

This IRP applies to all AI systems implemented by [Agency] Staff, contractors, and any entity operating on behalf of the [Agency]. The AI IRP addresses continuity and recovery procedures to appropriately mitigate AI incidents.

Approach

The key points in development of the AI IRP:

- Evaluate risk levels and determine the appropriate response for an AI incident, which may include obtaining senior management support.
- Keep the plan simple. A well-organized, systematic, and up-to-date AI IRP that is readily available will help teams get through most situations.
- Communicate regularly on the incident status. Provide the relevant facts as they are available, disseminate them quickly, follow up regularly, keep relevant parties informed and resolve incorrect information.
- Review.. The AI IRP must be reviewed at least bi-annually to ensure the documented procedures make sense and that the team is equipped to respond accordingly. Ensure an after-action plan is developed and communicated, with assigned improvement opportunities.
- Test. The AI IRP must be tested with tabletop exercises at least annually.
- Be flexible. The AI IRP should exhibit flexibility to meet a wide variety of situations, including team membership and access to appropriate resources. External partners such as law enforcement should be involved as needed.

AI Incident Response WG Deliverable: Response Plan Template

Purpose

1. Prepare and gain a fundamental understanding of the processes involved, the responsibilities, and the actions required to mitigate an AI incident.

2. Templatize the response plan to be applicable for each member agency.

What does the template cover?

1. Roles & Responsibilities
2. Activation Criteria
3. Response Level
4. Phased Approach & Preparation
5. Detection & Analysis
6. Containment
7. External Communications
8. Eradication & Recovery
9. Lessons Learned

AI Incident Response Plan WG Details

- The AI Incident Response Plan is based on the NIST AI Risk Management Framework and the Special Publication 800-61 Computer Security Incident Handling Guide.
- The scope of the plan covers internal and externally developed AI solutions.
- Definitions for harm and near harm serve as triggers for activation of the AIIR Plan
- The approach includes risk evaluation, regular communication, plan review and testing, and a simple and flexible plan to meet a wide variety of situations.
- The Preparation Phase includes a focus on end user awareness of current policies and post incident information sharing to prevent recurrence.
- The plan differentiates itself from other types of incidents that may have existing response plans, however it may be part of broader incidents related to cybersecurity, privacy, or other legal issues.

Vendor Agreements Working Group Update:

Standards and Requirements for AI Systems Template

Chairs:

- *Ethan Benatan (TriMet, OR)*
- *Ryan Kurtzman (Long Beach, CA)*

ADDENDUM X: STANDARDS AND REQUIREMENTS FOR AI SYSTEMS

This Addendum defines special requirements agreed to by [Agency] and Contractor regarding the AI systems and/or subsystems provided as part of the Contract.

AI Systems and subsystems governed by this Addendum include, without limitation, the following components:

- [list components here, the entirety or a subset of the software or services provided under the governing Contract]

Failure of the Contractor to comply with the terms of this Addendum shall constitute a material breach of the Contract. Contractor agrees to indemnify, defend, and hold harmless [Agency] regarding any third-party action rising out of or related to (1) any breach of any representation or warranty of Company contained in this Addendum; (2) any breach or violation of any covenant or other obligation or duty of Contractor under this Addendum or under applicable law; (3) any third party Claims which arise out of, relate to or result from any act or omission of the Contractor related to the provision of an AI System; and (4) any violations or alleged violations of intellectual property rights; in each case whether or not caused in whole or in part by the negligence of [Agency], or any other Indemnified Party, and whether or not the relevant Claim has merit.

1 AI SYSTEMS

"Artificial intelligence" or "AI" refer to any machine-based system that can, for a given set of human-defined objectives, make predictions, recommendations, or decisions influencing real or virtual environments.[1] Artificial intelligence systems use machine- and human-based inputs to perceive real and virtual environments; abstract such perceptions into models through analysis in an automated manner; and use model inference to formulate options for information or action.

An "AI system" is any data system, software, hardware, application, tool, or utility that operates

Vendor Agreements WG Deliverable: Standard Contractual Clauses for AI Systems

Purpose

1. Define AI-specific requirements for Vendors to follow when providing and/or operating AI systems to agencies.

2. Standard contractual language to be applicable for each member agency.

3. Complement existing contractual language (e.g., cybersecurity, privacy) to give agencies more teeth on AI-specific issues.

What does the template cover?

1. Risk Mitigation
2. Requirements for Contractors When Operating AI Systems
    1. Review
    2. Performance
    3. Algorithmic bias
    4. Human oversight
    5. Explainability
    6. Notice
    7. Incident Response
    8. Process
    9. Ongoing monitoring
    10. Training
    11. Auditing

Vendor Registry Working Group Update:

Registry Model & Intake Form

Chairs:

- *Roy Fernando (Cleveland, OH)*
- *Jiri Rutner (San Diego County, CA)*

Purpose

1. Provide the technology and platform for the GovAI Coalition to host and maintain information on AI tools for the public sector.

2. Accelerate the standardization and efficacy of AI solutions and their application to government services.

3. Create a knowledge base on the value AI products are bringing to public sector agencies.

Vendor Registry: *Summary of Model*

Vendor registers online, submits company details and AI FactSheet for models

Agencies report if they've used vendor's AI and can review experience

Use Case vignettes help agencies get started with use case

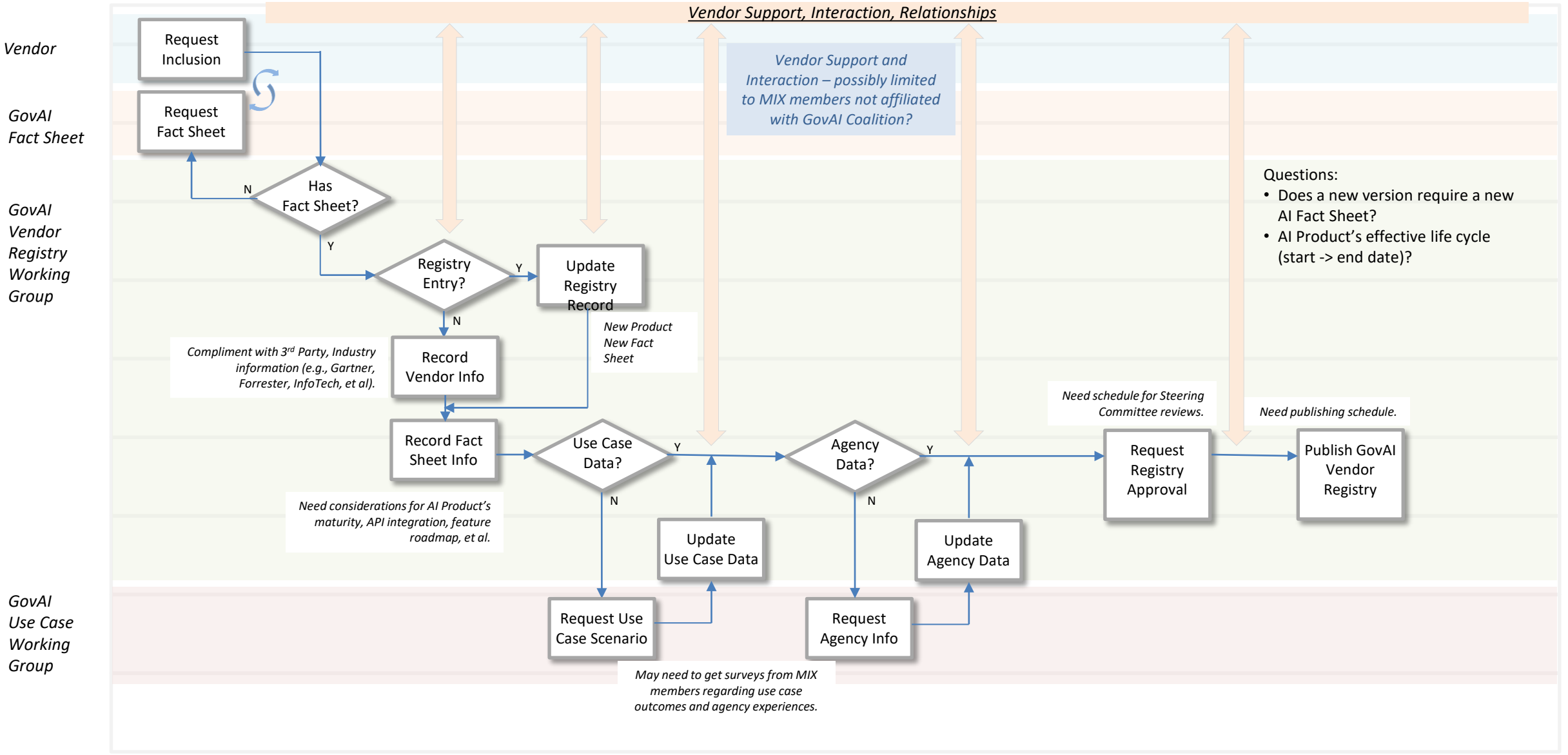
Vendor Registry

Agency-only view to see :

1. What vendors are transparent about re: their AI systems
2. Experiences with AI models from other agencies
3. Use Cases to do with these vendors and how to get started

Detailed: GovAI Vendor Registry Process Flow

GovAI – Vendor Registry Process Overview



Vendor Registry Intake Form Questions

Vendor Registry Intake Form Questions

General Vendor Information

1. Vendor Name
   (text)
2. How can government agencies reach you? Provide direct contact information or other means.
   (text)
3. What policies, if any do you have in place to ensure your AI system(s) is used responsibly? You detail below or provide a link
   (text)
4. Does your agency commit to the GovAI vendor pledge for responsible, accountable, and transparent AI systems?
   (Yes/No)
5. Would your company or service provider like to be included on the vendor registry?
   (Yes/No)

AI System specific information – Filled out per AI system

What counts as a system? Something that is sold as a packaged solution or product. For example, Azure's AI Translator service, Hugging Face's "Starcoder" text-to-code service, or LYT.ai Transit Signal Priority Service

1. What is the name of this AI system?
   (Text)
2. How long, in years, have you been providing this AI system?
   (Number)
3. In a sentence, what are the capabilities of this AI system?
4. (Text)
5. Is GenAI utilized for any aspect of the work performed by the AI system?
   (Text)
6. Have you provided this AI system to any other government agencies before? If yes, please list them with relevant contact information.
   a. Agency (text)
   b. Contact (text)
7. Attached is a copy of the GovAI Coalition AI FactSheet for vendors*. Please fill out and submit the form here for the AI system.
   (AI Factsheet attachment; includes: Vendor Name, System Name, Overview, Purpose, Intended Domain, Training Data, Test Data, Model Information, Update Procedure, Inputs and Outputs, Performance Metrics, Bias, Robustness, Optimal Conditions, Poor Conditions, Explanation, Jurisdiction-specific Consideration, Algorithmic Impact Assessment Questions)

DRAFT

Open Letter

Introduce and share outline

Value: United message

Goal: Align on Outline

/sanjoseca.sharepoint.com/:w:/r/sites/ITD_CollaborativeCityA
rementdocs/Shared%20Documents/General/General%20Coalition
cuments/240116%20Open%20Letter%20v2%20DRAFT.docx?d=we68
97bf4d119a9ee586a78ff4b9&csf=1&web=1&e=QWD4yi

Dear industry, policymakers, and the public,

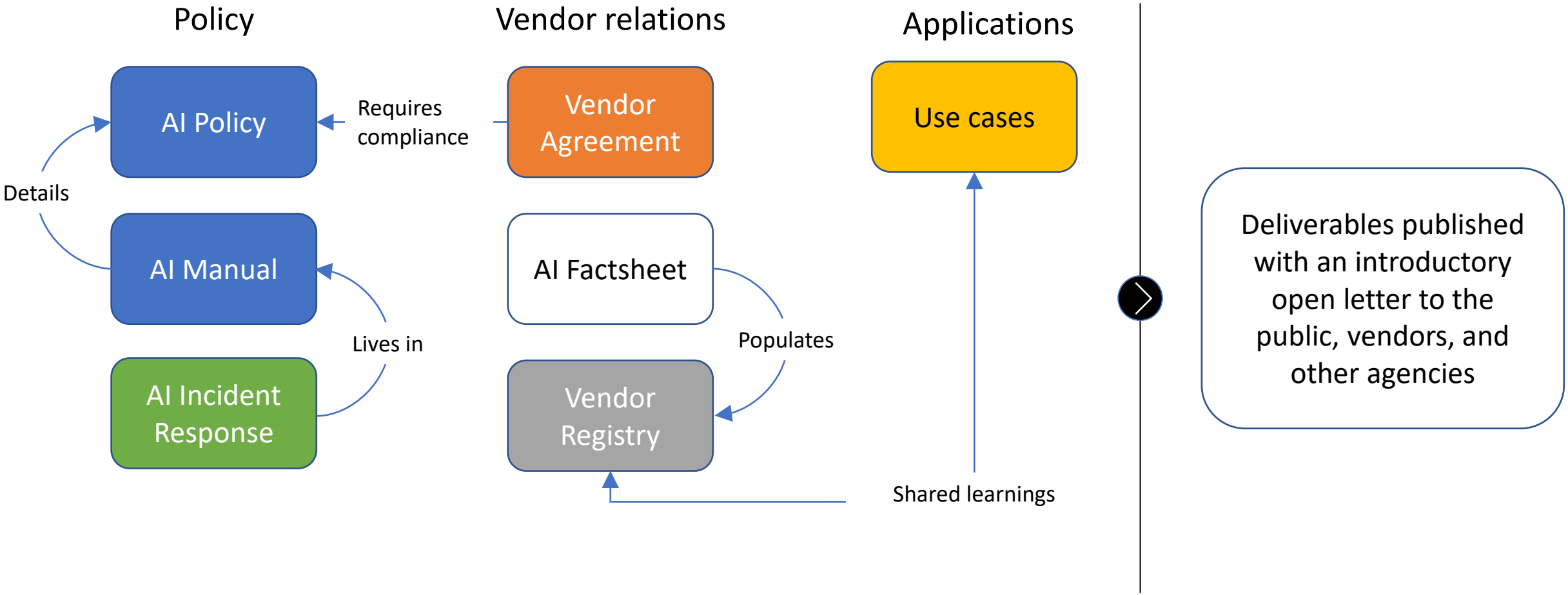
- **To the public: As a Coalition, we are committed to responsible AI practices.**
  - Our mission + goals
- **To vendors: As a Coalition, we demand greater accountability from vendors.**
  - AI FactSheet
  - Standard contractual clauses
  - Vendor Registry
- **To policymakers: As a Coalition, we advocate for the adoption of our released AI policy templates and practitioner documents by public agencies (or similar versions).**
  - AI Policy
  - AI Policy Manual
  - Use Cases template

Next steps

- Working groups iterate on templates; meet February
- Coalition meets February 29 at 1pm PT
- Coalition to vote on:
  - Working Group outputs (January and February)
  - Open letter to the public
- Interest in GovAI conference?

Appendix

GovAI - How do all the deliverables connect?



Phase I WGs: **Policy** | **Use Case** | **Vendor Registry** | **Vendor Agreement** | **Incident Response**