VIRGINIA IT AGENCY

Executive Order 30 and Artificial Intelligence (AI)

Agencies Information Session

Joshua Heslinga, Stephen Smith, Daniel Cherkis

May 22, 2024

Agenda

- Executive order 30 (EO 30) summary
- AI registration
- AI registration oversight
- AI registration secretary approval

Speakers and panel members

Speaker:
- Joshua Heslinga, *Director, Legal & Legislative Services*

Speaker:
- Stephen Smith, *Enterprise Architecture Manager*

Panel member:
- Daniel Cherkis, *IT Investment Management Consultant*

Executive Order 30 (EO 30)

- Issued on Jan. 18, 2024, building on reports and processes in Executive Directive 5 (9/20/2023).

- Puts in place standards and processes that aim to realize benefits of AI while mitigating risks:
  - Policy standard sets forth guiding principles and measures to mitigate risks and protect the data of Virginians, including disclaimers and a mandatory registration and approval process for uses of AI.
  - Technology standard provides protocols and requirements for use of AI.
  - Education and law enforcement will have distinct guidelines and considerations, developed by SecPSHS and OAG.
  - An AI task force will be created to provide ongoing recommendations.

- Copies of EO 30 and the policy and technology standards may be found on VITA AI webpage: https://www.vita.virginia.gov/artificial-intelligence/

Definitions

- **Executive Branch Agency (found in EO 30):**
  Any agency, institution, department, board, bureau, commission, council, public institution of higher education, or other instrumentality of state government in the Executive Department as listed in the Appropriations Act.

- **Artificial Intelligence (found in the technology standard):**
  The simulation of human intelligence processes by machines, especially computer systems, such that it can <u>adapt and learn on its own</u> using machine learning algorithms that can analyze large volumes of training data to identify correlations, patterns, and other metadata that can be used to develop a model that can make predictions or recommendations based on future data inputs.

  - *This definition excludes:* technologies like robotic processes, data search, software automation and workflows, programmable devices, application software, and optimization programs.

AI Policy and Standards

Utilization of AI by COV Policy Standard	AI Standard (Enterprise Architecture)
▪ **Ethical use** — AI solutions must be resilient, accountable and explainable; AI models must be documented; AI outcomes must be validated by humans for bias ▪ **Business cases** — AI must produce a positive outcome for Virginians and be the optimal solution for the outcome ▪ **Mandatory registry & approvals** — Each use of an AI solution must be recorded in a central AI registry and, after vetting by the agency, reviewed for approval by VITA and the responsible Secretary. ▪ **Mandatory disclaimers** — Public disclosure when AI is used to produce a decision or output, including how decisions were produced ▪ **Risk mitigation** — AI & vendor vetting / risk assessment required for procurement and use of AI ▪ **Protect citizen data** — Prioritize privacy & data protection, especially for sensitive & confidential data. Notification and required consent when using citizen data. Data retention and minimization required.	▪ **Safety** — AI systems must be employed in such a way that as to win public trust and cause no harm to people, businesses or the environment ▪ **Accountability** — Risks associated with COV decisions must always remain with humans to avoid potential bias and discrimination by AI systems ▪ **Data Security & Privacy** — Data collected, leveraged or trained in an AI system must be controlled, secured, and untraceable back to an individual ▪ **Transparency** — Use of AI solutions in COV systems must be clear as to their use, extent and value ▪ **Sustainability** — Building and fostering skills that will support COV into the future and not lead to automation complacency or de-skilling

Tool set definition

- **Archer:**
  Commonwealth of Virginia (COV) risk management system where the AI Registry information is entered and managed.
  - It is recommended for ISOs to manage records via Archer
  - Access will be available for entities that require registration – agencies who need access to Archer should send an email to commonwealthsecurity@vita.virginia.gov
    - *Requested subject line: <School name> - Archer access*

- **Commonwealth technology portfolio (CTP):**
  CTP is the tool used to track AI registration approvals.
  - For those without CTP access send an email to ITIMD@vita.virginia.gov with the AI registration PDF document
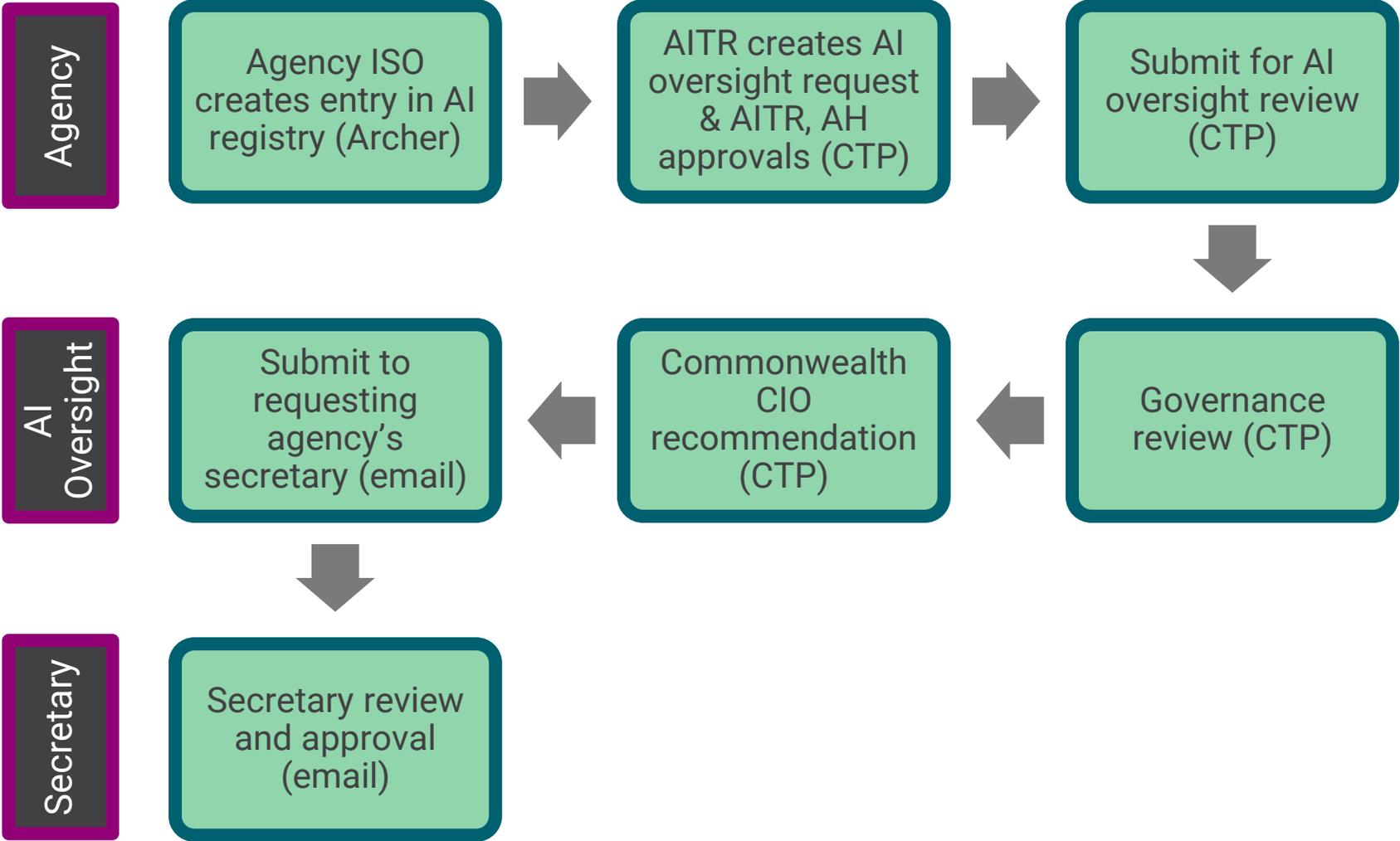
AI submission

Within the Archer application agencies will be prompted to submit the following details regarding their applications:

- Artificial Intelligence type
- Purpose
- Sensitivity
- Public Safety
- Technology Used
- Model Architecture
- Model Input
- Model Output Data Type & Structure
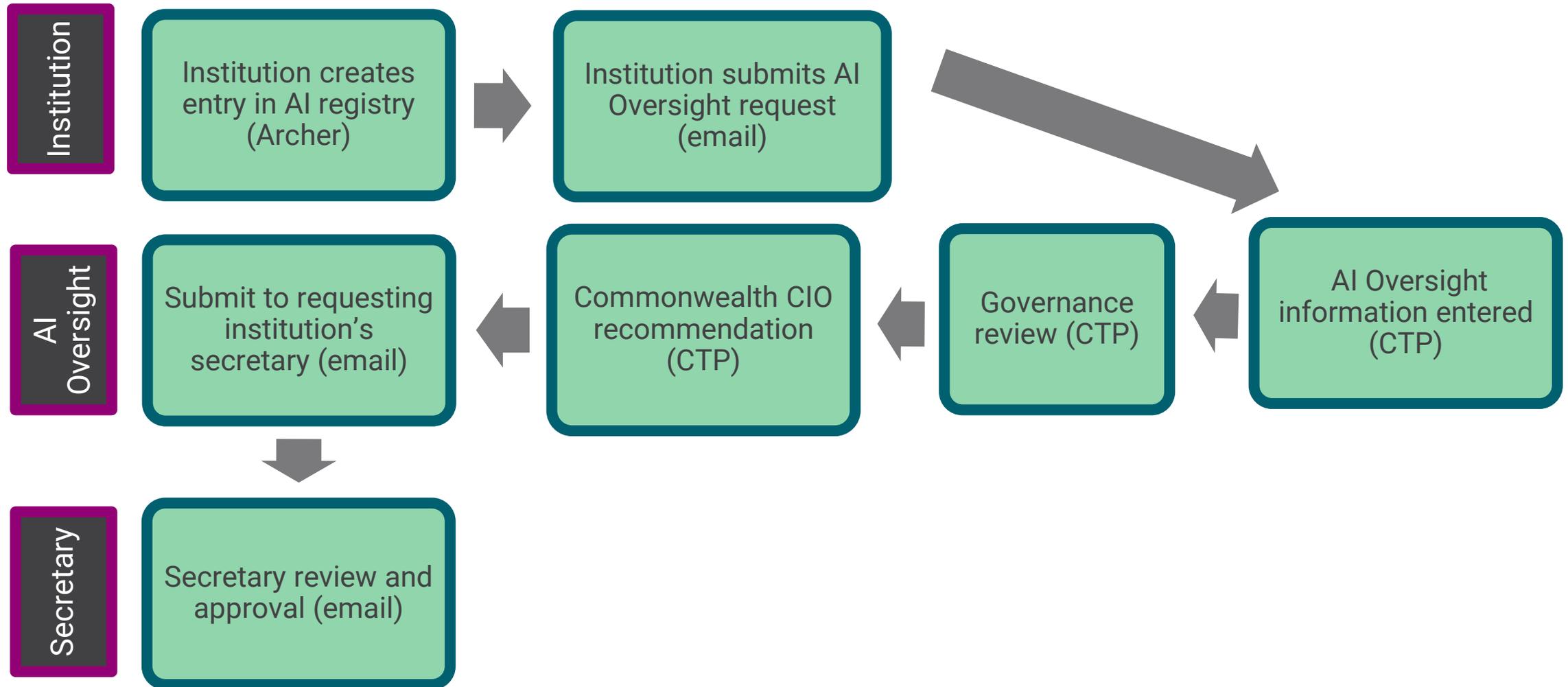- Model Algorithm
- Data Sets used
- Operation

When submitting for approval the following details will be collected:

- Proponent secretary
- Proponent agency
- Is this new or existing AI software?
- Existing AI Software in Service Date

AI registration and approval workflow (those who use CTP)

Agency

Agency ISO creates entry in AI registry (Archer) → AITR creates AI oversight request & AITR, AH approvals (CTP) → Submit for AI oversight review (CTP) ↓

AI Oversight

Submit to requesting agency's secretary (email) ← Commonwealth CIO recommendation (CTP) ← Governance review (CTP)

Secretary

Secretary review and approval (email)

AI registration and approval workflow (those who do not use CTP)

Institution

Institution creates entry in AI registry (Archer) → Institution submits AI Oversight request (email) → AI Oversight information entered (CTP)

AI Oversight

Submit to requesting institution's secretary (email) ← Commonwealth CIO recommendation (CTP) ← Governance review (CTP) ← AI Oversight information entered (CTP)

Secretary

Secretary review and approval (email)

VIRGINIA
IT AGENCY

vita.virginia.gov *Email itimd@vita.virginia.gov for status updates*

Frequently asked questions

What is the process for applications that require COV Ramp (previously known as ECOS)?

Will I need to register AI technology internally such as Microsoft CoPilot?

Will applications in use before EO 30 was enacted need registration?

Available resources:

- [Registering AI job aid (those with CTP access)](#)
- [Agency head job aid](#)
- [Higher education AI registration process](#)
- Coming soon:
  - Frequently asked questions and answers from this info session

Questions?
Thank you!