INFORMATION POLICY AND PROCEDURE
OFFICE OF INFORMATION & TECHNOLOGY MANAGEMENT

Artificial Intelligence (AI) Strategy & Procedures	
Information Policy Number: AI0001	
Approval Date: 03/04/2026	Next Review Date: 03/04/2028

Issued by the Chief Information Officer (CIO)

JAMES TUNNESSEN Digitally signed by JAMES TUNNESSEN Date: 2026.03.04 11:01:38 -05'00'

James Tunnessen
Chief Information Officer/Chief AI Officer
National Endowment for the Arts

ARTIFICIAL INTELLIGENCE (AI) STRATEGY & PROCEDURES

Revision History

Version 0.9 – June 5, 2024: Initial policy memo created for comment period.
Version 1.0 - September 6, 2024: Initial Document Approved
Version 2.0 – August 27, 2025: Document revised to align with Presidential Directives
Version 2.1 – March 4, 2026: Added language from M-26-04

1. PURPOSE

This document establishes the National Endowment for the Arts (NEA)Artificial Intelligence (AI) Strategy & Procedures in accordance with Executive Order 14179, Accelerating Federal Use of AI through Innovation, Governance, and Public Trust.

2. BACKGROUND

AI has the potential to help the government mitigate fraud, reduce errors, and lower the cost of paper-intensive processes, while enabling collaboration across multiple divisions and agencies to provide more effective and efficient services to citizens. There are many types of AI with numerous use cases in which the government can benefit. Some of the more common AI tools that are used in commercial and government practice include: Generative AI, Virtual Personal Assistants, Chatbots, Recommendation Systems, Image Recognition, Automated Translation, and Automated Transcription. These types of AI tools utilize specialized types of AI such as Natural Language Processing (NLP), Machine

Learning (ML), and Deep Learning. By safely harnessing these tools, the NEA can significantly impact both business processes as well as provide the foundational capabilities to achieve the objectives that fulfill the strategic goals of the organization.

As AI technologies advance, NEA must continually assess the opportunities and potential risks associated with their uses to ensure that NEA can effectively leverage emerging technologies to achieve its missions.

---

3. AUTHORITY

- Executive Order 14179, Accelerating Federal Use of AI through Innovation, Governance, and Public Trust (January 23, 2025)
- Executive Order 13859, Maintaining American Leadership in Artificial Intelligence (February 11, 2019)
- Executive Order 13960, Promoting the Use of Trustworthy AI in the Federal Government (December 3, 2020)
- Clinger-Cohen Act of 1996, Public Law (PL) 104-106
- Code of Federal Regulations (CFR), Title 5, Administrative Personnel, Part 930 Subpart C, "Information Security Responsibilities for Employees who Manage or Use Federal Information Systems"
- Directive 1901, "Privacy Management", February 2019
- Directive 1910, "Information Management", February 2019
- E-Government Act of 2002, PL 107-347, Title III, "Federal Information Security Management Act (FISMA)", as amended
- FIPS 199, "Standards for Security Categorization of Federal Information and Information Systems", February 2004
- FIPS 200, "Minimum Security Requirements for Federal Information and Information Systems", March 2006
- The Federal Information Security Modernization Act (FISMA) of 2014, PL 113-283, December 2014
- Freedom of Information Act (FOIA), 5 United States Code (USC) § 552, as amended by PL 104-231, 110 Stat. 3048, "Electronic FOIA Amendments of 1996"
- NIST SP 800-53, Revision 5, "Security and Privacy Controls for Information Systems and Organizations", September 2020
- NIST SP 800-70, Revision 4, "National Checklist Program for Information Technology (IT) Products: Guidelines for Checklist Users and Developers", February 2018
- Office of Management and Budget (OMB) Circular A-130, "Managing Information as a Strategic Resource", July 2016
- OMB Memorandum M-26-04, "Increasing Public Trust in Artificial Intelligence Through Unbiased AI Principles", December 2025
- OMB Memorandum M-25-21, "Accelerating Federal Use of AI through Innovation, Governance, and Public Trust", April 2025
- OMB Memorandum M-25-22, "Driving Efficient Acquisition of Artificial Intelligence in Government" April 2025

- OMB Memorandum M-06-16, "Protection of Sensitive Agency Information", June 2006
- OMB Circular No. A-119, "Federal Participation in the Development and Use of Voluntary Consensus Standards and in Conformity Assessment Activities
- Paperwork Reduction Act of 1995, 44 USC 3501-3519
- Privacy Act of 1974, 5 USC § 552a, as amended

---

4. RELATED DOCUMENTS

Related policies and procedures are available on the NEA's OITM Policy Resources SharePoint site. These additional resources include the following examples:

- Awareness and Training Policy and Procedures
- Information Security Policies and Procedures
- Risk Assessment Policy and Procedures
- Security Assessment and Authorization Policy and Procedures
- System and Information Integrity Policy and Procedures
- Supply Chain Risk Management Policy and Procedures

---

5. SCOPE AND APPLICABILITY

The scope of the AI Strategy & Procedures includes OITM's review, approval, and allowed implementation of the use of AI tools to aid in the business processes used to achieve the NEA's mission.

---

6. AUDIENCE

The audience is anyone who uses information systems that are maintained or supported by the NEA.

---

7. REVIEWS AND UPDATES

NEA shall review this document, as appropriate, but at least once every two years, and update it as necessary.

8. ROLES AND RESPONSIBILITIES

a. Chief Information Officer (CIO)

1) The CIO is responsible for:
   ~~a.~~ Filling the role of the agency's Chief Artificial Intelligence Officer to ensure overall compliance with the agency's AI policy and federal AI policies and mandates
   b. Coordinating with the agency's Chief Information Security Officer (CISO) to ensure that all planned AI implementations meet the agency's information security requirements
   c. Coordinating with the agency's Chief Privacy Officer (CPO) to ensure that all planned AI implementations meet the agency's privacy requirements
   d. Coordinating with the agency's Chief Data Officer (CDO) to ensure that all planned AI implementations meet the agency's data requirements
   e. Approving the development, use, and implementation of AI products, tools, and algorithms and providing the Authority to Operate as the agency's Authorizing Official;
   f. Overseeing the integration of AI systems with existing IT infrastructure;
   g. Ensuring data integrity and security;

b. Chief Artificial Intelligence Officer (CAIO)

1) The CAIO is responsible for:
   a. Serving as the senior advisor for AI to the head of the agency and other senior agency leadership and within the agency's senior decision-making forums;
   b. Instituting the requisite governance and oversight processes to achieve compliance with the Federal government's guidance on the responsible use of AI;
   c. Working with and advising the CFO on the resourcing requirements necessary to implement a successful and effective agency AI initiatives and providing recommendations on priority investment areas to build upon existing enterprise capacity;
   d. Advising the Chief Human Capital Officer (CHCO) and where applicable, the Chief Learning Officer, on improving workforce capacity and securing and maintaining the skillsets necessary for using AI to further the agency's mission and adequately manage its risks;
   e. Sharing relevant information with agency officials involved in the agency's major AI policymaking initiatives;
   f. Supporting agency involvement with appropriate interagency coordination bodies related to the agency's AI activities, including representing the agency on council described in Executive Order 14179;
   g. Supporting and coordinating the agency's involvement in AI standard-setting bodies, as appropriate, and encouraging agency adoption of voluntary consensus standards for AI, as appropriate and consistent with OMB Circular No. A-119;
   h. Work with the agency to identify and prioritize appropriate uses of AI that

will advance both their agency's mission

i. Identify and remove barriers for the responsible use of AI in the agency, including the advancement of AI-enabling enterprise infrastructure, data access and governance, workforce development measures, policy, and other resources for AI innovation;
j. Establish and chair an agency AI Council ensuring diverse representation from across the agency's offices;

c. **Chief Information Security Officer (CISO)**

1) The CISO is responsible for:
   a. Ensuring the security of AI systems, including data encryption, access controls, and review systems with regular security audits;
   b. Managing risks from the use of AI systems;

d. Chief Privacy Officer (CPO)

1) The CPO is responsible for:
   a. Safeguarding sensitive information and ensuring compliance with privacy regulations, including protecting PII during the use of AI;

e. Chief Data Officer (CDO)

1) The CDO is responsible for:
   a. Managing data quality, ensuring data governance policies are followed, and overseeing the integration of AI-generated content with other datasets;
   b. Ensuring data formats meet the requirements necessary for the agency's proposed AI initiatives;

f. Chief Financial Officer (CFO)

1) The CFO is responsible for:
   a. Providing the resourcing requirements necessary to implement successful and effective agency AI initiatives and help recommend priority investment areas to build upon existing enterprise capacity;
   b. Assessing the expected benefits, such as increased efficiency, cost savings, and improved decision-making, against upfront and ongoing costs or implementing AI technologies;
   c. Collaborating with the CIO and CAIO to establish financial governance frameworks for AI initiatives;

g. Director of Human Resources

1) The Director of Human resources is responsible for:
   a. Working with the CAIO on improving workforce capacity and securing and maintaining the skillsets necessary for using AI to further the agency's mission and adequately manage its risks;
   b. Ensuring equitable access to AI training opportunities and training staff on the

appropriate use of AI;
c. Addressing any concerns about job displacement;

h. Agency Ethics Officer

1) The Agency Ethics Officer is responsible for:
   a. Evaluating the ethical implications of AI usage;
   b. Providing guidance on ethical decision-making;
   c. Addressing ethical concerns raised by NEA staff;

i. Director of Equal Employment Opportunity and Civil Rights (EEO)

1) The Director of EEO is responsible for:
   a. Ensuring the AI usage does not result in discrimination or bias;
   b. Addressing any complaints related to equal employment opportunity and civil rights violations regarding AI initiatives;

j. AI Council

1) The AI Council is responsible for:
   a. Establishing and maintaining an agency AI Use Case Inventory which will be posted on the OITM SharePoint site;
   b. Establishing and/or updating processes to measure, monitor, and evaluate the ongoing performance and effectiveness of the agency's AI applications and whether the AI is advancing the agency's mission and meeting performance objectives;
   c. Establishing controls to ensure that the agency does not use AI that is not in compliance with Federal government regulations such as M-25-21;
   d. Providing strategic guidance on the use of AI technologies;
   e. Evaluating potential risks and benefits of using AI;
   f. Recommending policies to mitigate any identified risks associated with the use of AI;
   g. Submitting AI technologies to the agency's CIO for an Authority to Operate within the agency's technology environment

---

9. POLICY

The CAIO will facilitate the responsible advancement of AI innovation within the NEA. Doing so, the NEA will improve its ability to use AI in ways that benefit the public and increase mission effectiveness, while recognizing limitations and risks of AI and when it is not suited for a given task. The CIO/CAIO will convene an AI Council to effectively review and plan implementation of AI solutions within the organization.

9.1 AI Council

The AI Council will be chaired by the Chief Artificial Intelligence Officer and at a minimum will consist of these key stakeholders or their designated representatives:

- Chief Information Officer/Chief Artificial Intelligence Officer (Chair)
- Chief Information Security Officer
- Chief Privacy Officer
- Chief Financial Officer
- Chief Data Officer
- Director of Human Resources
- Agency Ethics Officer
- Director of Equal Employment Opportunity and Civil Rights
- Deputy Chairman for Programs and Partnerships

9.2 AI Use Cases

NEA staff are encouraged to provide AI use cases to the CAIO for review. These use cases should provide insight into how the agency will benefit by the implementation of the AI solution into the NEA work environment. The CAIO will initiate the review process (noted in the *Procedures* of this document) of the AI technology and provide an approved or disapproved response as to the use of the technology within 90 days from the request starting Phase 2 of the review process. Use case requests should be completed using the attached *Artificial Intelligence Use Case Request* in Appendix A and should be submitted through CAIO@arts.gov with the following subject line **AI Use Case: Name of Technology**.

9.3 Unapproved and Disapproved AI Technology

Unapproved AI technology is technology that has not yet received approval or disapproval for use through the AI Council. A Use Case may or may not have been provided for review.

Disapproved AI technology is technology that has been disapproved by the AI Council and is not authorized for use by NEA staff members. A Use Case was provided to the AI Council and disapproved for use within the NEA or the proposed AI conflicts with the M-26-04 and does not meet the Administration's two Unbiased AI Principles: Truth-Seeking and Ideologically Neutral. In accordance with the memorandum,

> "**Truth-seeking:** LLMs shall be truthful in responding to user prompts seeking factual information or analysis. LLMs shall prioritize historical accuracy, scientific inquiry, and objectivity, and shall acknowledge uncertainty where reliable information is incomplete or contradictory."
>
> *"**Ideological Neutrality:** LLMs shall be neutral, nonpartisan tools that do not manipulate responses in favor of ideological dogmas. Developers shall not*

intentionally encode partisan or ideological judgements into an LLM's outputs unless those judgements are prompted by or otherwise readily accessible to the end user."

NEA staff members will not use unapproved or disapproved AI technology during their work within the NEA. Not adhering to this policy could lead to the improper use of AI tools causing proprietary and personal data leakage and unintentionally introducing malicious software into the NEA technical environment.

Use of unauthorized or disapproved AI may result in appropriate sanctions, including but not limited to remedial training; verbal or written warning; loss of access to information systems; loss of a security clearance; termination of employment; or civil or criminal prosecution.

9.4 Conditionally Approved AI Technology

The Office of Information & Technology Management (OITM) actively explores use cases for AI tools across a variety of NEA offices. This work is continuous and the CIO/CAIO has determined that the NEA must enable and encourage NEA personnel to responsibly use commercial products to harness the benefits of AI and ensure the agency continuously adapts for the future of work. The following guidance is to facilitate appropriate use during this early stage of AI technological development:

- OITM in coordination with the AI Council will develop and maintain a list of conditionally approved and approved commercial AI tools for use in the NEA. Conditionally approved commercial AI tools are approved for use on open-source/public information only.

- In developing these lists, OITM will work with the AI Council and will review basic accuracy and security practices, supply chain risk management concerns, privacy and civil liberties safeguards, and available information on how training data was sourced.

- OITM will maintain a page on the OITM SharePoint site listing these tools and offering employees the ability to submit additional tools for review and testing.

OITM will update Agency IT and cybersecurity policies and standards to include new requirements for use of approved AI tools by NEA personnel in their work. While an AI tool is under conditional approval the following rules shall apply:

- Personnel must never put NEA data regarding individuals (regardless of whether it is personally identifiable information (PII) or anonymized), social media content, or any For Official Use Only, Controlled Unclassified Information (CUI), or Classified information into the AI tool.
- Personnel shall protect any PII collected or generated by commercial AI tools in accordance with applicable NEA privacy policy and federal law.
- Before using these tools, personnel must get approval from their supervisors, complete a training on responsible use of AI along with their annual Privacy and Cybersecurity Awareness trainings, and sign an acknowledgement of conditions

of use.

- Personnel will create accounts on these tools using their NEA email and use these accounts for NEA use, separate from any personal use of these tools.
- Personnel will select options in tools that limit data retention and opt out of inputs being used to further train models.
- All use of conditionally approved commercial AI tools will be on the web, not through downloaded desktop or mobile apps.
- Personnel are always accountable for accessing and handling NEA information and IT resources in compliance with NEA User Rules of Behavior and NEA policies, including privacy, civil rights, and civil liberties policies.
- Personnel should ensure all content generated or modified using these tools is reviewed by appropriate subject matter experts for accuracy, relevance, data sensitivity, inappropriate bias, and policy compliance before using it in any official capacity, especially when interacting with the public.
- Conditionally approved AI tools may not be used in the decision-making process for any grant awards, benefits adjudication, credentialling, vetting, law or civil investigation or enforcement related actions. Agency and Office Leaders can request from the CIO's office a written waiver of these restrictions.
- Any spillage or compromise of NEA information into conditionally approved AI tools must be reported to security@arts.gov immediately pursuant to applicable policies.

9.5 Engaging with the Public

When engaging with NEA stakeholders, the NEA staff member will ensure that unapproved and disapproved AI is not used during the meeting that includes discussing personal or proprietary data. The NEA staff member will request that any unapproved and disapproved third-party AI solution be disabled prior to those meetings. A constituent's or panelist's failure to comply will result in the cancelation and rescheduling of the meeting to a time when the constituent or panelist has agreed not to use the third-party AI solution.

9.6 Human in the Loop

Immediate appropriate applications for commercial AI tools in the NEA business could include generating first drafts of documents such as Statements of Work, policies, procedures, conducting and synthesizing research on open-source information, providing automated transcription and translation, and developing briefing materials or preparing for meetings and events. However, AI technologies may be prone to "hallucinate" (provide false information) or biased results which may negatively impact business operations if they are left unchecked. This policy requires that the NEA adopt the best practice of having a staff member fact-check and correct the data or documentation and review and correct any AI influenced documents displaying any biased or discriminatory implications prior to publishing.

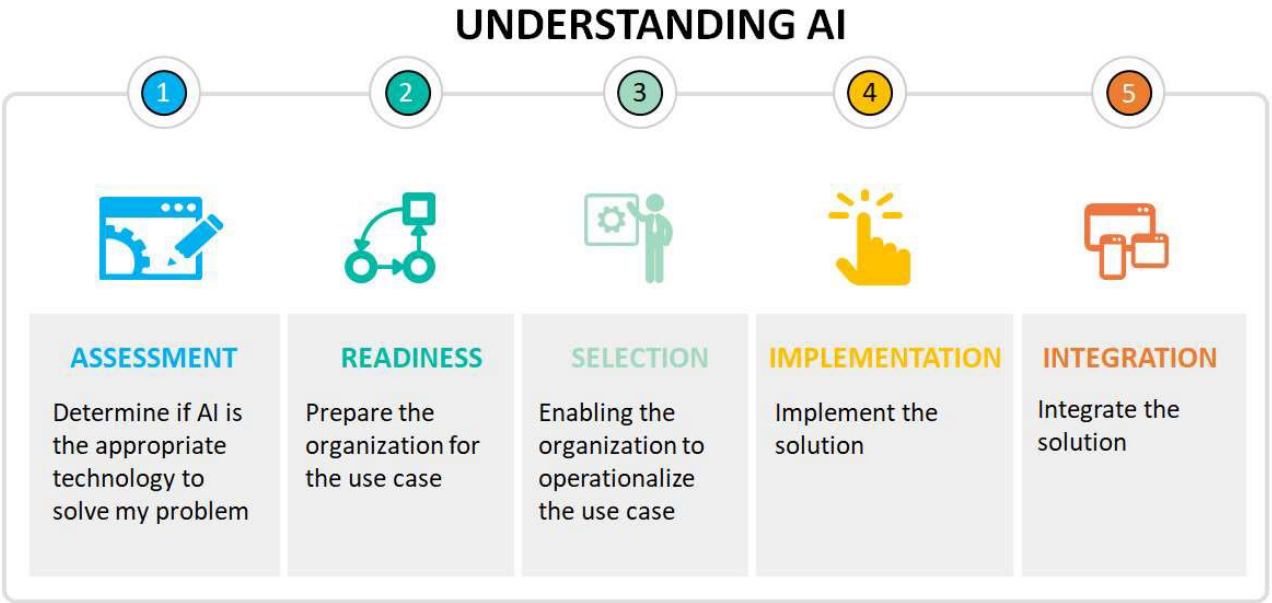
9.7 Intellectual Property

AI services, especially those based upon generative AI technology, are typically "trained" by their providers on voluminous datasets, and often also allow end users to input datasets themselves when entering prompts. Upon entering a textual or other prompt in an AI service, a user prompts the AI service to generate a work or works based upon the dataset training the service has received. Because such datasets may contain/utilize publicly available data/works subject to or protected by copyright and other intellectual property (IP) rights, both the input into and generation of works via AI services can raise IP infringement considerations depending upon the circumstances. Further, the use (e.g., copying, distribution, display, creation of derivatives) of works generated via AI services can likewise raise IP infringement considerations depending upon the circumstances. When utilizing AI services in an official capacity, Agency personnel are not to input into AI services (whether through user prompts or datasets) any content protected by copyright or other IP rights absent appropriate permission from the relevant rightsholders. Because an AI generated work is not typically accompanied by any attribution to the party that produced it or any information as to the inputs entered into the AI service by the producing party, NEA personnel are not to use AI service generated works produced by third parties (e.g., AI service generated works appearing on third-party websites).

---

10. PROCEDURES

AI technology could provide several solutions and provide an evolutionary catalyst to solve and support the evolution and transformation of the entire organization. The CAIO will create an Agency AI Council consisting of key stakeholders across the agency to help provide direction, guidance, evaluation, and the successful implementation of Agency AI solutions. The CAIO and AI Council will participate in the decision-making steps outlined in this policy and procedures.



10.1 Understanding the Agency AI Decision-Making Process

The agency will follow a 5-phase decision-making process in the evaluation and

introduction of AI technologies.

Phase 1 – Problem Assessment/Use Case Development: Develop a vision and business objectives through various assessments to ensure the AI solution addresses a specific use case and delivers results that optimize services and operational delivery.

Phase 2 – Organizational Readiness: Engage AI subject matter experts and consider the nuances that accompany an AI solution to prepare the organization. The AI Use Case is presented to the AI Council where they review the functional and technical requirements, and implementation plans. The identified AI solutions go before the OITM CCMB to review the technical, cybersecurity, and integration requirements for deployment in the NEA technical environment.

Phase 3 – Solution Selection: The AI Council conducts a thorough investigation of business consideration, types of AI requirements, deployment models, and procurement options to enable optimal provider selection to achieve the desired end state.

Phase 4 – AI Implementation: Customize and configure AI solution to meet the organization's operational objectives.

Phase 5 – AI Integration: (*Hand off to OITM and HR)* Integrate AI solution into the organization's infrastructure and provide the necessary training to integrate into the organization's business practices.

a. Phase 1 – Problem Assessment/Use Case Development

Phase 1 is designed to help decision makers create the most value through their AI initiative. Staff members identify operations areas that could be improved through AI through drafting Use Cases. The Use Case is presented in a document demonstrating the problem, assessing the need for AI, and indicating how the implementation of an AI technology will create a more efficient and effective work environment.

- Key Goals
  - Determine if AI is the appropriate technology solution
- Key Participants
  - The NEA staff member requesting the AI solution

b. Phase 2 – Organizational Readiness

The purpose of this phase is to prepare enterprises and organizations for AI efforts and define key supporting activities to ensure organizational readiness. At this stage, the AI Requester presents their AI Use Case to the AI Council. The AI Council reviews the Use Case presented and provides analysis and feedback. The Use Case is then forwarded to OITM to go through the CCMB for technical evaluation and feedback. These committees review and discuss the nuances specific to the proposed AI that should be considered prior to the organization taking on the initiative. After it has been reviewed by both committees it is either Approved or Disapproved for use within the NEA. The form is then filed in the Artificial Intelligence folder on the OITM

SharePoint site which is available to all NEA staff members.

Key Goals

- Assess risks and establish risk mitigation strategies through AI Council review of the AI technology
- Analyze selected key performance indicators (KPI) strategies through AI Council review of the AI technology
- Ascertain existing systems' integration readiness through CCMB review and sign off on the AI technology
- CAIO approval or disapproval of the use of the proposed AI technology

- Key Participants

  - The NEA staff member requesting the AI solution
  - AI subject matter experts (SME) who may or may not be from the agency initiating the program
  - AI Council
  - Members of the CCMB

c. Phase 3 – Solution Selection

Selection comes after the Readiness Phase and the organization has determined that it has the necessary requirements to implement an AI solution. This phase focuses on selecting the right tools, policies, people, etc., for a successful implementation of AI technology.

- Key Goals
  - Selection of the right AI technology for the use case.
  - Understanding the NEA's capabilities to support AI implementation.
  - Aligning the NEA's acquisition strategy with the high-value AI solutions.

- Key Participants
  - Vendors for review of AI technologies
  - AI Council reviewing the presented AI technologies
  - CFO for funding
  - OITM members to understand implementation methods and requirements
  - Contracting Officer

- Key Outcomes
  - Business stakeholder SMEs and enterprise architects are engaged in developing a scalable solution.
  - Business architecture and changes to the business processes are defined and agreed upon.
  - Clear identification of the boundary for process automation and analysis of the impact on the overall business processes
  - Mitigation plans are in place for the following risk categories:
    - Technology
    - Business Processes
    - People
    - Security

        - Performance
        - User Experience
        - Adoption
        - Regulatory compliance
        - Enterprise integration

    - KPIs are defined and baselined for the selected business case (use case)
    - Enterprise-level platform architecture is defined to scale up the solution in future, if needed
    - Implementation controls like estimated budget, schedule, master plans, and required type of resources are planned and programmed
    - A procurement strategy is defined and coordinated with the acquisition community

d. Phase 4 – AI Implementation

In the Implementation Phase, the inner workings of the selected solutions are completed and tested. It closely examines the technical implementation of AI components and the operational aspects, such as governance and security posture, to ensure the optimal operations of the AI solution.

- Key Goals
    - Take the models, processes, and technologies determined in the previous phases and implement them so they can be integrated within the organization in the next phase.
    - Conceptual technical architecture developed with a tested proof of concept
    - Data sources identified
    - High level diagram of the business architecture is drafted including the business process, business rules, technology, roles, and responsibilities
    - Identification and description of AI funding streams, workforce requirements, business initiatives, technical system dependencies are collected in a Resource Plan

- Key Participants (*may vary based on the project*)
    - Business Process Owner
    - IT Project Manager
    - Chief Artificial Intelligence Officer
    - Chief Data Officer
    - Data Scientists
    - Enterprise Architect
    - Software Developers
    - Machine Learning Engineers
    - Testers

- Key Outcomes
    - Obtain an Authority to Operate (ATO) or Authority to Use (ATU)
    - Conduct a Proof-of-Concept (Pilot)

e. Phase 5 – AI Integration

Once the NEA has gone through Readiness, Assessment, Solution Selection, and AI Implementation phases successfully, this next phase integrates the AI solution into the organization's infrastructure.

- Key Goals

  The key goal of this phase is to get the AI solution, processes, strategies developed and implemented in the previous phases and integrate them into the organization that will operate and maintain the AI solution.

- Key Participants

  - Product owners/managers to undertake overall management and governance of proposed AI solution
  - AI SMEs who are integrating the program
  - Stakeholders from the lines of business and systems with technical, process, or data intersections or integration with the proposed AI solution
  - An enterprise architect who is well versed with AI and data architectures to lead the execution of the integration framework into a production model capability
  - Change process leader driving change management:
    - Configuration planning
    - Item identification
    - Change control
    - Configuration status accounting
    - AI/ML configuration audit
  - Executive Sponsor: CIO

10.2 Acquisition

NEA will use the acquisition process, if applicable, to gather information from vendors that will assist with identifying and mitigating risks from the use of AI, including but not limited to:

- **Intended use** – Vendors should identify uses that are suitable for their AI and purposes, contexts, and uses that are not suitable for their AI's use;
- **Training data** – Vendors should provide details about the model's training data, including the source of the data, the time periods the data describes, and the extent to which the data reflects real-world contexts. For training data that reflects populations, vendors should provide summary statistics of the population whose data it was trained on that are relevant to a public benefits context (e.g., race/ethnicity, age, gender, income brackets).
- **Testing results** – Vendors should provide information about how they have tested their system, what contexts they tested it in, findings from their testing, and changes they made to address any issues discovered during the testing process.
- **Audit results** – Vendors should disclose whether the system and data have been assessed for automation bias and/or other risks, the results of any assessments, and any actions taken to mitigate findings.

NEA should only acquire and use AI if a vendor provides all necessary information to evaluate suitability and risk. Purchasing from GSA or NASA SEWP acquisition schedules may simplify the process of gathering information if disclosure is required by the schedule's terms and conditions.

NEA should consider acquisitions that enable the agency to try AI technologies before committing to expensive or lengthy contracts. Agencies could consider testing the technology in a controlled, isolated environment known as a sandbox or conducting a limited pilot to evaluate suitability, risks, and gains from using AI.

Note: As AI becomes more commonplace, NEA should anticipate that vendors may respond to proposals with solutions containing AI, even if AI features were not requested or anticipated for that acquisition.

10.3 Responsible Data Use

Despite best efforts to mitigate errors and protect rights, situations will arise where AI does not perform as expected and creates unacceptable risk or harm, such as an AI chatbot that provides incorrect information about program eligibility to the public or an AI-enabled routine in a management information system that begins to produce biased outcomes. AI-enabled functions should be able to be disabled without creating unacceptable disruption to service delivery. NEA should be able to disable AI functions quickly in response to an identified unacceptable risk or harm through system settings, feature flags, or other actions that do not require new development or redeployment of a system.

Staff should be trained in fallback processes that do not rely on AI-enabled functions.

---

11. WAIVERS/RISK ACCEPTANCE

Waivers or Risk Acceptance may be requested from the CIO by submitting a justification based on:

- Substantive business case needs
- Demonstration of, or a proposal for, establishment of adequate compensating controls that provide a suitable alternative to the mandated protection

The CIO may grant a waiver or risk acceptance for sufficient reasons, exercising judgment, in the best interests of the NEA. Waivers and risk acceptance must be reviewed, revised, and approved annually.

The CISO shall coordinate to maintain a central repository of all waivers and risk acceptances.

---

12. DEFINITIONS

1. Artificial Intelligence: Any artificial system that performs tasks under varying and unpredictable circumstances without significant human oversight, or that can learn from experience and improve performance when exposed to data sets; an artificial system developed in computer software, physical hardware, or other context that solves tasks requiring human-like perception, cognition, planning, learning, communication, or physical action; an artificial system designed to think or act like a human, including cognitive architectures and neural networks; a set of techniques, including machine learning, that is designed to approximate a cognitive task; an artificial system designed to act rationally, including an intelligent software agent or embodied robot that achieves goals using perception, planning, reasoning, learning, communicating, decision making, and acting.

2. Automation Bias: The propensity for humans to inordinately favor suggestions from automated decision-making systems and to ignore or fail to seek out contradictory information made without automation.

3. Generative AI: Algorithms used to create new content such as audio, code, images, text, and videos. These systems fall under the broader category of machine learning, which uses training data to generate rules that produce outputs. Generative AI can create new content based on learned patterns rather than predefined content and patterns from humans.

4. Natural Language Processing (NLP): A specialized type of AI that enables the understanding and generation of human language by machines. It is used in various AI tools like chatbots and automated translation systems.

5. Machine Learning (ML): A subset of AI involving algorithms and statistical models that enable computers to perform tasks without explicit instructions by relying on patterns and inference. It includes predictive models used to observe and classify patterns in data.

6. Deep Learning: A specialized type of machine learning involving neural networks with three or more layers. These networks attempt to simulate the behavior of the human brain to "learn" from large amounts of data.

7. AI Hallucinations: The phenomenon where AI systems produce invented and inaccurate responses. This risk is significant in Generative AI tools and requires careful human oversight to ensure accuracy and relevance of the outputs.

6. Conditionally Approved AI Tools: AI tools approved for use on open-source/public information only. They are under review for basic accuracy, security practices, supply chain risk management, and compliance with privacy and civil liberties safeguards.

7. Unapproved AI Technology: AI technology that has not yet received approval or disapproval for use through the AI Council. It includes technology for which a Use Case may or may not have been provided for review.

8. Disapproved AI Technology: AI technology that has been reviewed and explicitly

disapproved by the AI Council, making it unauthorized for use by staff members.

9. Human in the Loop: A best practice approach where a human fact-checks, corrects, and reviews AI-generated or influenced data and documents to ensure accuracy, relevance, and absence of bias before final use.

APPENDIX A

Artificial Intelligence Use Case Request
To be completed by the AI tool Requester

Date:

Submitter:

Office:

Statements

Problem to be solved:

Technology presented:

Current Business Process in place:

Business Value/Outcome by introducing AI process:
Please describe the expected outcome of the implementation of this AI technology. Gains in productivity and potential cost savings should be addressed.

AI Questions

1) Is there sufficient data available and identified for the Use Case?
    a. What data?
    b. Does the data contain metainformation?
    c. Are the authoritative data sources of the Use Case organized, structured, deconflicted, and matriculated?
2) Is there a predictive element to the Use Case?
3) Have other technologies been applied successfully to address elements of the Use Case?
4) Could the result of the Use Case change how conformance requirements need to be applied? (E.g., personally identifiable information [PII], CUI, etc.)
5) Does the Use Case contain ethical considerations and is there a potential for bias?

AI Council Evaluation of Use Case
To be completed by the AI Council

1) Is the data available and complete?

2) How mature is the AI technology presented?

3) Compliance Assessment:

    a. Legal considerations (*ethical*):

    b. Privacy considerations:

    c. Cybersecurity considerations:

    d. Human capital considerations:

    e. Financial considerations:

4) Is this technology already deployed within the agency?

    a. Where?

    b. For what?

    c. Are there lessons learned to be shared?

5) Will the organization benefit from this technology as represented in this Use Case?

6) Can the agency use this technology in other areas or business lines? If so, which ones and how?

CCMB Review
To be completed by the OITM

Enterprise Architecture Review:

Cybersecurity Review:

Infrastructure Review:

Application Development Review:

IT Services Support Review:

Approval
To be signed off by the CIO/CAIO

AI Technology for Use Case Approved: _____

AI Technology for Use Case Disapproved: _____

Reason for Disapproval:

CIO/CAIO Signature

Date: _____

Name: _____

Title: _____

Signature: _____

** Use Case Template to be available all NEA staff and filed on the Artificial Intelligence Folder on the OITM SharePoint Site following this title format:*
use_case_title using name_of_technology date