NEA Compliance Plan for OMB Memoranda M-24-10 September 2024

Prepared by Chief AI Officer Jim Tunnessen

1. STRENGTHENING AI GOVERNANCE

General

NEA is committed to the safe, secure, responsible, and trustworthy use of AI. On April 17, 2024, NEA assigned the duties and title of the Chief Artificial Intelligence Officer to the Chief Information Officer. NEA has developed an enterprise policy and procedures, *Use of Artificial Intelligence Policy and Procedures*, to provide an overarching framework for advancing AI innovation and AI governance while managing the risks from the use of AI. This document reflects the guiding principles required in OMB M-24-10 *Advancing Governance Innovation and Risk Management for Agency Use of Artificial Intelligence*, March 28, 2024.

NEA intends to enhance the workforce through the delivery of AI functions that will provide greater efficiency and effectiveness to the operations of the agency's grant making process. To do this, the NEA has established an AI Council overseen by the CAIO. The AI Council consists of members from across the agency with expertise to assess risk and promote effective and responsible AI use within the agency.

AI Governance Body

NEA has established a governance structure to approve and oversee the review, implementation, and use of AI at the agency through the NEA AI Council. The CAIO serves as the Chair. Key members of the AI Council consist of senior officials or delegates within the agency that cover technology, privacy, cybersecurity, data, civil rights, equity, human capital, budget, legal, and program management.

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: Integrate AI solution into the organization's infrastructure and provide the necessary training to integrate into the organization's business practices.

Throughout the AI decision-making process, developing safe and effective AI products and services requires a dedicated team with a wide-ranging set of skills and expertise, including data scientists, cloud specialists, analysts, designers, and domain experts. AI projects are reviewed and approved at each stage of the development process by the CAIO and the NEA AI Council.

AI Use Case Inventories

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 with the NEA AI Council (noted in the NEA *Use of AI Policy and Procedures*) 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 *Artificial Intelligence Use Case Request* and submitted to the CIO/CAIO office to initiate review.

As AI projects move through the NEA's AI Decision-making Process from Phase 3 – Solution Selection to Phase 4 – AI Implementation, they will be added to the NEA's AI Use Case Inventory if they meet the criteria for inclusion pursuant to OMB guidance, as determined by the CAIO. NEA will publish the version of the NEA AI Use Case Inventory incorporating the 2024 updates in alignment with the December 16, 2024, deadline provided by OMB.

All AI systems are required to adhere to stringent guidelines to maintain their Authority to Operate (ATO) status, ensuring continuous compliance and oversight. The CIO/CAIO will maintain an Approved, Conditionally Approved, and Disapproved AI tool list.

AI Use Cases not subject to inventory

NEA will assess if an AI product may be excluded from NEA's AI Use Case Inventory in accordance with EO 14110. NEA will continue to review the AI projects and use cases through the AI Decision-making Process. AI products in production will be reviewed annually and AI use cases that were previously excluded from public reporting will be reevaluated annually by the CAIO for determination as to whether it should be added to NEA's published inventory.

2. **ADVANCING RESPONSIBLE AI INNOVATION**

Removing Barriers to the Responsible Use of AI

NEA is embracing innovation in the development of its IT infrastructure to account for the addition of AI tools to enhance the Agency's workforce. A development environment is being created to provide a testing area and opportunities to pilot AI technologies before they are deployed en masse to the NEA staff. The agency will ensure that all AI tools go through the CCMB review process to ensure that technical, interconnections, data, and cybersecurity concerns are addressed prior to deployment. Data collections with planned integrations into AI solutions will be reviewed and tested prior to agency release to assess quality, representativeness, and bias.

Generative AI's immediate appropriate applications 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 NEA *Use of Artificial Intelligence Policy and Procedures* requires that the NEA adopt the best practice of having staff members 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. The policy provides specific requirements and use limitations designed to safeguard data and protect privacy. The policy also lays out a process for obtaining approval to use Generative Ai tools or commercially available AI tools which includes the completion of cybersecurity training respective to the AI tool requested and agreeing to follow rules of behavior when using these tools.

NEA aims to promote responsible and effective use of AI technologies and solutions within the agency.

AI Talent

NEA intends to use the government-wide direct hire authority for Information Technology Specialists; Computer Scientist (Artificial Intelligence); Computer Engineers (Artificial Intelligence); and Management and program Analysts in the grade levels GS-9 through GS-15 as necessary in building up the AI talent of the agency.

In order to increase the NEA employees' AI skillset, NEA is encouraging the agency staff to take advantage of the Gov2Gov AI training provided by OPM. NEA is also providing agencywide AI tool demos and training as well as providing commercially available self-paced AI training videos.

For recruitment, NEA will target skillsets including data science, data visualization, and machine learning engineers to aid in the workflow processes and data reporting analysis and reporting requirements for the agency.

AI Sharing and Collaboration

The NEA AI Council will review custom developed AI code, models, and data and share them with the public when legally permissible in accordance with M-24-10. NEA actively collaborates with other government agencies, academic institutions, and research institutions to promote the exchange of information and resources. NEA fosters a culture of openness and collaboration among the internal offices and external agencies which will drive advancements in AI technology and its applications.

Harmonization of Artificial Intelligence Requirements

NEA has developed the *Use of Artificial Intelligence Policy and Procedures* which provide specific guidelines on how to request a Use Case, the steps the Use Case will go through for approval, and how it will be implemented and integrated into the workforce if approved. This document is available on the NEA's Office of Information & Technology Management's internal website. This provides a consistent methodology for AI Use Case review and implementation. NEA has put in a two-year review period for the policy and procedures and will continue to refine the process to improve AI tool delivery to the NEA workforce.

3. MANAGING RISKS FORM THE USE OF ARTIFICIAL INTELLIGENCE

Determining Which AI is Presumed to be Safety-Impacting or Rights Impacting

NEA will 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.

NEA distinct criteria to guide a decision to waive one or more of the minimum risk management practices for a particular use case is as follows:

> 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.

Implementation of Risk Management Practices and Termination of Non-Compliant AI

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. Technology that is not approved will be blocked and immediately uninstalled from the network.

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.

Minimum Risk Management Practices

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. The goal is to assess risks and establish risk mitigation strategies through AI Council review of the AI technology.