Title: IT Governance of Artificial Intelligence and Autonomous Systems (AI/AS)
Policy Tracking#: TSI-19-XX
Effective Date:
Originating Office: Office of the Chief Information Officer (OCIO) (202)-384-8680

(a) PURPOSE: In recognition of the increasingly pervasive role of algorithmic decision-making systems in corporate and government service and growing public concerns regarding the black-box nature of many of these systems, USAGM Chief Executive Officer (CEO), Office of Chief Council (OGC) and Chief Information Officer (CIO) have established within this policy an initiative on the procurement, use, data management, ethics and cybersecurity requirements for the use of Autonomous and Intelligence Systems to meet agency Strategic Goals and Objectives. This policy aims to provide the framework for the development of Automated Decision Systems (ADS), Artificial Intelligence (AI), Autonomous Systems (AS) and Machine Learning (ML) technology capabilities[1] procedures for each acquired capability to include comprehensive staff training. In addition, it lays the out a platform for the adoption and use of new standards and solutions, certifications and codes of conduct, and consensus building for ethical implementation of intelligent technologies. For the purpose of this policy and users, the acronym ADS/AI will be used to define all such capabilities.

(1) Advance an agency discussion about how we can establish ethical and social implementations for intelligent and autonomous systems and technologies, aligning them to defined values and ethical principles that prioritize human well-being in a given cultural context.

(2) Inspire the creation of Standards (IEEE P7000™ series and beyond) and associated certification programs.

(3) Facilitate the emergence of national, federal and global policies, standards and conformance metrics are integrated and align with USAGM's set of seven overarching Governance of ADS/AI Principles.

(i) Governance of ADS/AI Principles:

(A) **Principle 1** — Organizational Governance: Provide sufficient oversight into the internal/external impact assessments, governance, ethics, and accountability of the use of these technologies around the agency, within public/private sector agreements and established service level agreements

(B) **Principle 2** — Human Rights: Ensure the use of these technologies do not infringe on local, national, and internationally recognized human rights

(C) **Principle 3** — Prioritizing "Human-in-the-Loop": Ensure during the use of these technologies the command chain that authorizes the use is documented and approved

[1] The use of the acronym AI/AS in this policy refers to the following holistically: Artificial Intelligence (AI), Autonomous Systems (AS) and Machine Learning (ML) technology capabilities

to the extent where the commands flow down to a human to support specific actions and/or task

(D) **Principle 4** — Accountability: Ensure that within the procurement documentation and server level agreements (SLAs) that the designers and operators are responsible and accountable throughout the life cycle of the technology

(E) **Principle 5** — Transparence: Privacy, and Data Management: Ensure these technologies operate in a transparent manner, meet federal privacy and data management requirements as these technologies and use evolves

(F) **Principle 6** — ADS/AI Technology Misuse and Awareness: Minimize the Strategic, Operational, and technical risks of their misuse

(G) **Principle 7** — ADS/AI Cybersecurity Eco-system(s) Requirements: Ensure the organization is protected and the architecture of such technologies are transparent to all leadership, include top-down bottom-up empowerment, ownership, and responsibility, and the need to consider system deployment contexts

(b) To ensure that USAGM use of ADS/AI technologies best serves our interest as well as the public we serve, USAGM leadership believes that effective ADS/AI policy and supporting capability procedures should embody a rights-based approach that achieves *Seven* principal objectives:

1. Support, promote, and enable national and internationally recognized legal norms

2. Develop a workforce expertise in ADS/AI technology to ensure "Human-In-The-Loop" when using ADS/AI Technologies

3. Include ethics as a core competency in the use of ADS/AI technology while researching and developing USAGM products and services

4. Explore options for assessing accuracy and the potential for bias in ADS/AI data and algorithms

5. Regulate the procurement and use of ADS/AI to ensure agency and public safety and establish agency-wide as well as public/private sector partners responsibilities.

6. Educate the USAGM employees and contractors on societal impacts of use of ADS/AI technologies to meet agency strategic initiatives, goals and objectives

7. Ensure the most up to date cybersecurity capabilities are acquired and staff are trained as part of the total cost of ownership with procuring ADS/AI technology

(c) AUTHORITY & SCOPE:

(1) Authorities.

(i) Executive Order “Maintaining American Leadership in Artificial Intelligence & Technology Issued on: February 11, 2019

(ii) Federal Information Security Modernization Act (FISMA) of 2014, Public Law 107-347

(iii) Framework for Improving Critical Infrastructure Cybersecurity

(iv) The National Technology Transfer and Advancement Act (NTTAA); Public Law 104-113 National Technology Transfer and advancement act of 1995; Including Amendment by Public LAW 107-107, section 1115 on Dec 28 2001. Utilization of Consensus Technical Standards by Federal Agencies

(v) Office of Management and Budget (**OMB**), OMB A-119; : Federal Participation in the Development and Use of Voluntary Consensus Standards and in Conformity Assessment Activities, Revised January 2016

(vi) Office of Management and Budget (OMB) Circular A-130, Section 8b(3), ―Securing Agency Information Systems,‖ as analyzed in A-130, Appendix IV: Analysis of Key Sections. Supplemental information is provided in A-130, Appendix III.

(vii) Federal Acquisition Regulation (FAR)

(viii) Cloud Smart Strategy, October 2018

(ix) Federal Risk and Authorization Management Program (FedRAMP)

(2) **National and International Consensus Based Standards**. The agency uses national and international consensus based standards in accordance with OMB A-119, to ensure the agency has established the appropriate standard of care associate with ADS/AI technologies:

(i) FIPS Publication 199, Standards for Security Categorization of Federal Information and Information Systems;

(ii) FIPS Publication 200, Minimum Security Controls for Federal Information Systems;

(iii) NIST SP 800-30, Risk Management Guide for Information Technology Systems

(iv) NIST SP 800-37, Guide for the Security Certification and Accreditation of Federal Information Systems;

(v) NIST Draft SP 800-39, Managing Risk from Information Systems: An Organizational Perspective;

(vi) NIST SP 800-53, Recommended Security Controls for Federal Information Systems;

(vii) NIST SP 800-53A, Guide for Assessing the Security Controls in Federal Information Systems; and

(viii) NIST Special Publication 800-60 Volume II, Revision 1, Volume II: Appendices to Guide for Mapping Types of Information and Information Systems to Security Categories

(ix) NIST SP 800-122 — Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)

(x) NIST 800-161 – Supply Chain Risk Management Practices for Federal Information Systems and Organizations

(xi) Department of Commerce Grants and Cooperative Agreements Manual

(xii) NIST Policy 5700.00 Managing Public Access to Results of Federally Funded Research

(xiii) IEEE P7000™ - Model Process for Addressing Ethical Concerns During System Design

(xiv) IEEE P7001™ - Transparency of Autonomous Systems

(xv) IEEE P7002™ - Data Privacy Process

(xvi) IEEE P7003™ - Algorithmic Bias Considerations

(xvii) IEEE P7004™ - Standard on Child and Student Data Governance

(xviii) IEEE P7005™ - Standard on Employer Data Governance

(xix) IEEE P7006™ - Standard on Personal Data AI Agent Working Group

(xx) IEEE P7007™ - Ontological Standard for Ethically driven Robotics and Automation Systems

(xxi) IEEE P7008™ - Standard for Ethically Driven Nudging for Robotic, Intelligent and Autonomous Systems

(xxii) IEEE P7009™ - Standard for Fail-Safe Design of Autonomous and Semi-Autonomous Systems

(xxiii) IEEE P7010™ - Wellbeing Metrics Standard for Ethical Artificial Intelligence and Autonomous Systems

(xxiv) IEEE P7011™ - Standard for the Process of Identifying and Rating the Trustworthiness of News Sources

(xxv) IEEE P7012™ - Standard for Machine Readable Personal Privacy Terms

(xxvi) IEEE P7013™ - Inclusion and Application Standards for Automated Facial Analysis Technology

(xxvii) Artificial Intelligence & Cybersecurity for Dummies, IBM Limited Edition, by Ted Coombs

(3) **Scope**. This policy provides guidance to all USAGM staff, contractors, and public/private sector partners on procuring and managing ADS/AI technologies, their associated ICT supply chains--ecosystems, and potential risks to the agencies reputation while using these technologies to create agency products and services. The processes and controls described in this policy build on federal agency guidance and are shaped to guide implementation. While public/private sector partners outside of the USAGM may decide to consult this publication as a source of good practices, the policy does not contain any specific guidance for those entities. That guidance will be added to Grantee agreements moving forward.

The guidance and internal controls in this policy are required for use with all acquired and maintained ADS/AI technologies according to Federal Information Processing Standard (FIPS) 199, Standards for Security Categorization of Federal Information and Information Systems [FIPS 199]. However, because of interdependencies and individual needs, USAGM may choose to apply the guidance to systems at a both High-impact as well as lower-impact level and to very specific ADS/AI system components in order to avoid any risk from unknown black-box architectures.

USAMG shall carefully consider the potential costs of applying ADS/AI technologies internal controls beyond high/low impact information systems and weigh the costs against the risks to the organization of not applying boundary specific ICT SCRM controls. This policy also applies to the acquisition and migration to Cloud Service (i.e. ADS/AI/ML) As-as-Service and consult with OGC with all Service Level Agreements (SLAs) prior to acquiring the technology. Implementing these controls will require financial, human and training resources, not just from the agencies directly but also potentially from their systems integrators, suppliers, and external service providers that would also result in increased costs to the acquirer. ADS/AI ICT SCRM controls support risk management and should be considered in the context of the agency's or partner's unique missions, geographic location, local laws, internal operational environments, and enterprise risks. In applying this policy, supporting procedures/processes and internal controls, USGAM leadership may decide to include requirements that they include in other policies, acquisition guidelines, and procurement documents.

(d) POLICY:

(1) USAGM CEO; OGC, CO, CIO Council CIO's and Partners, Directors of VOA, TSI, OCB; and its own subordinate Directors and Managers of Divisions and Services will collaboratively support the governance of; the procurement, use, legal ramifications, privacy, intellectual property rights, human rights, and cybersecurity requirements

(2) A key component of this policy is the requirement to develop an Agency-wide ADS/AI procedures for each procured capability

(3) The Agency shall develop an agency-wide staff training to ensure A/IS Technologies are not Misused and all users have Awareness that promotes safety, privacy, intellectual property rights, human rights, and cybersecurity requirements

(e) PRIMARY RESPONSIBILITIES:

(1) The CEO and Director shall act to ensure/monitor the overall strategic direction of the procurement, use, safety, privacy, intellectual property rights, human rights, and cybersecurity requirements ADS/AI technologies across all parts of the Agency.

(2) The CEO; Directors of VOA, TSI, OCB; and its own subordinate Directors and Managers of Divisions and Services shall:

(i) Be held accountable to the Principles and Standards of Care established within this policy and any supporting procedure associated with the use of ADS/AI technologies

(ii) CEO; Directors of VOA, TSI, OCB; and its own subordinate Directors and Managers of Divisions and Services shall assign one or more of its own personnel to take part as member of its own

(iii) Directors of VOA, TSI, OCB; and its own subordinate Directors and Managers of Divisions and Services (s) shall:

(A) Validate (an auditable artifact) the ADS/AI Architecture. These technologies are often opaque (frequently referred to as "black boxes") and create difficulties for everyone, from the engineer, to the lawyer in court, to the social media user. The results is an abundance of ethical issues of ultimate accountability. There is the potential for USAGM users of A/IS will not be aware of the sources, scale, varying levels of accuracy, intended purposes, and significance of uncertainty in the operations of A/IS, or that they are interacting with A/IS in the first place. The sources of data used to perform these tasks are also often unclear. Furthermore, users might not foresee the inferences that can be made about them or the consequences when

A/IS are used. The proliferation of A/IS will result in an increase in the number of systems that rely on machine learning and other developmental systems whose actions are not pre-programmed, and that may not produce logs or a record of how the system reached its current state.

(B) Systems for registration and record-keeping should be created so that it is always possible to find out who is legally responsible for a particular A/IS. Manufacturers/operators/owners of A/IS should register key, high-level parameters, including:

(1) Intended use

(2) Training data/training environment (if applicable)

(3) Sensors/real world data sources

(4) Algorithms

(5) Process graphs

(6) Model features (at various levels)

(7) User interfaces

(8) Actuators/outputs

(9) Optimization goal/loss function/reward function

(C) Establish Level of Autonomy Description for each ADS/AI Capability describing the Level of automation effects on performance, situation awareness and workload in a dynamic control tasks as follows:

(1) Manual Control: Human monitors, generates options, makes decisions, and physically carries out options.

(2) Action Support: System assists human with execution of selected action. Human performs some control actions.

(3) Batch Processing: Human generates and selects options; turns them over to the system to carry out (e.g., cruise control in automobiles).

(4) Shared Control: Human and System both generate possible decision options. Human has control to select which options to implement; carrying out the options is a shared task.

(5) Decision Support: System generates decision options that human can select. Once option is selected, system implements it.

(6) Blended Decision Making: System generates option, selects it, and executes it if human consents. Human may approve of the option selected by the system, select another, or generate another option.

(7) Rigid System: System provides set of options and human must select. Once selected, system carries it out task and/or associated defined activities.

(8) Automated Decision Making: System selects and carries out option. Human can have input in the alternatives generated by the system.

(9) Supervisory Control: System generates options, selects, and carries out desired option. Human monitors and intervenes if needed (in which case the level of autonomy becomes Decision Support).

(10) Full Automation: System carries out all actions. System itself decides if human intervention is needed.

(11) Directors of VOA, TSI, OCB; and its own subordinate Directors and Managers of Divisions and Services must also consider three components of supervised autonomy: ‘direction’ (telling it what to do), ‘monitoring’ (watching what it is doing), and ‘control’ (being able to intervene and change what it is doing).

(D) Must establish Principles for Accountable Algorithms and a Social Impact Statement for Algorithms when using ADS/AI technologies to meet USAGM mission needs.

(1) Principles for Accountability of Algorithms and Social Impact should include at a minimum the following:

(i) **Responsibility**: Externally visible avenues of redress for adverse individual or societal effects and designate an internal role for the person who is responsible for the timely remedy of such issues.

(ii) **Explainability**: Ensure that algorithmic decisions as well as any data driving those decisions can be explained to end-users and other stakeholders in non-technical terms.

(iii) **Accuracy**: Identify, log, and articulate sources of error and uncertainty so that expected and worst-case implications can be understood and inform mitigation procedures.

(iv) **Auditability**: Enable interested third parties to probe, understand, and review the behavior of the algorithm through disclosure of information that enables monitoring, checking, or criticism, including through provision of detailed documentation, technically suitable APIs, and permissive terms of use.

(v) **Fairness**: Ensure that algorithmic decisions do not create discriminatory or unjust impacts when comparing across different demographics (e.g. race, sex, etc).

(iv) Chief Information Officer (CIO) and CIO Council: As these technologies are integrated into the USAGM workplace, the CIO and CIO Council will:

(A) Establish a strategy, measure your organization against the AI maturity model.

(1) This model can be used as a framework to identify where your organization is on the potential growth curve, communicate with management and decide what steps need to be taken.

(2) Ensure that Directors of VOA, TSI, OCB; and its own subordinate Directors and Managers of Divisions and Services ADS/AI Strategies are highly adaptive, with ample room for experimentation, test and evaluation, and corrective action.

(i) Ensure ADS/AI pilot projects or experiments are taking place prior to fulling launching these capability's

(ii) Ensure meetings about ADS/AI focus on knowledge sharing and the beginnings of standardization conversations.

(iii) Ensure at least one ADS/AI project has moved to production and best practices, and experts and technology are accessible to the enterprise.

(iv) Ensure ADS/AI technologies has an executive sponsor and a dedicated budget.

(v) During FY IT budget calls, all new digital projects at least consider ADS/AI, and new products and services have embedded ADS/AI. Employees in process and application design understand the technology. ADS/AI-powered applications interact productively within the organization and across all business ecosystem.

(B) Look for critical business points where human interaction or human expertise adds value.

(C) Find examples where such value is manifested

(1) In very large amounts of data,

(2) Where the data includes the outcomes that they desire to affect

(3) Where customer interactions record whether the customer's experience was positive

(D) Consider how AI might augment those efforts to create even more value.

(v) Chief Information Security Officer (CISO), shall:

(A) Ensure USAGM's investments in ADS/AI capabilities include the requisite cybersecurity needs to achieve cyberhygiene and enforce least privilege environments at scale.

(B) Since FedRAMP still requires Department of Homeland Security (DHS)—Cybersecurity and Infrastructure Security Agency (CISA) and OMB direction on the acquisition of ADS/AI Cloud Services, CISO will be required to develop internal CIO approved accreditation processes for Authorization-to-Operate (ATO).

(C) Development, maintenance, and testing of internal and Cloud Service Provider ADS/AI technologies.

(D) Regular review annually the USAGM Information Security Architecture to ensure acquired ADS/AI technologies are embedded.

(E) Each Cloud Service Provider should assure USAGM CISO that its key suppliers—supply chain or partners which support a critical ADS/AI activity have effective physical and cybersecurity capabilities in place.

(3) Strategy

(i) In order to meet the requirements of our customers and stakeholders while supporting the USAGM mission; "*to insure we continue to inform, engage and connect people around the world in support of freedom and democracy*" USAGM will procure, establish awareness and training to secure our investments in ADS/AI technologies for our workforce.

(4) Communication, Staff Training and Awareness. To increase awareness around ethical issues in the realm of intelligent and autonomous systems, USAGM Training Division along with the supporting Directors of VOA, TSI, OCB; and its own subordinate Directors and Managers of Divisions and Services; develop an agency-wide Communication, Staff Training and Awareness program to support USAGM's procurement of ADS/AI technologies

(5) Training, Testing, After Action, and Maintenance.

(i) Training. It is mandatory for employees to take part in regular ADS/AI training activities and its own Service Area to ensure team training and exercising implemented as required. Organizing such training or testing is the responsibility of the Directors of VOA, TSI, OCB; and its own subordinate Directors and Managers of Divisions and Services for service area ADS/AI or its own delegated representative. The training shall take place at a time when its effect on our customers or clients is minimal.

(ii) Rehearsals. To make the continued use of ADS/AI effective, regular testing is required to ensure proper responses and actions are taken when and if an ADS/AI incident should occur. The results of the tests in the form of a corrective action plan shall be reported to the CEO, OGC and CIO in case of unsatisfactory results, the reasons are determined, and alterations may be made to the relevant part of the service area ADS/AI Crisis Management Plan.

(iii) Operational Shortfalls and Limitations. All parts of the Agency shall prioritize and provide its own list of ADS/AI operational shortfalls and limitations in the annual Agency-wide Budget Office data call for Capital Planning and Investment Control (CPIC) funding consideration.

(iv) After-Action Program. Directors of VOA, TSI, OCB; and its own subordinate Directors and Managers of Divisions and Services shall have a corrective action documented process which should follow a review of its own unit-specific ADS/AI program, plans, processes and procedures, staff training and follow an actual event or exercise to identify program deficiencies, and take necessary corrective actions to address such deficiencies.

(v) ADS/AI incident response process deficiencies should be identified within one or more of the overarching Business Continuity, and Disaster Recovery planning frameworks (i.e. Annexes and supporting Appendixes). Corrective actions should be identified by using the following Six categories:

(A) Human Resources (Human-In-The-Loop);

(B) Plan(s) or SOPs revisions;

(C) Training, actual event/disruption and exercises;

(D) Equipment, IT additions or modifications, facility requirements, and funding needs

(E) ADS/AI Architecture/Ecosystem—Supply Chain validation and changes; and

(F) Cybersecurity ADS/AI Security and Contingency Plans, and Authorization to Operate (ATO)

(6) Maintenance. To keep the ADS/AI suite of plans up-to-date and current, alterations may be necessary when procedural changes to service operations occur or when new threats/risks

arise; therefore, the maintenance of the business impact and recovery ability analysis and ADS/AI contingency plans is an ongoing annual process.

(7) Review Process. Periodic testing of processes and procedures are required to assess a continuity/contingency plan’s effectiveness and the organization’s readiness to execute it.

(i) Key service area Business Continuity and IT Contingency, Incident Response, and Disaster Recovery Plans shall be completed as soon as possible and reviewed annually to ensure that information on service functions, contacts and telephone information are kept up to date. In addition a program of testing and exercising shall be developed.

(ii) Any lessons learned from actual events, training, exercising or request for change shall be incorporated into the rolling annual review process and placed on the Agency intranet.

(8) Audit and Governance. ADS/AI arrangements form part of the Agency’s overall auditable internal controls environment, which are subject to annual review by the Department of State (DoS) Inspector General, CEO, OGC, CIO and the Board of Governors.

(f) DEFINITIONS:

(1) For the purposes of this policy, the term “Agency” means all bureaus, offices, and divisions of the Federal Government supervised by the Chief Executive Officer (CEO).

(2) Artificial Intelligence (AI): (December 12, 2017 (H.R. 4625 and S. 2217)), defined AI as follows: “Any artificial system that performs tasks under varying and unpredictable circumstances, without significant human oversight, or that can learn from their experience and improve their performance.... They may solve tasks requiring human-like perception, cognition, planning, learning, communication, or physical action.”

(3) Autonomous Systems (AS): An autonomous system is a collection of connected Internet Protocol routing prefixes under the control of one or more network operators on behalf of a single administrative entity or domain that presents a common, clearly defined routing policy to the internet.

(4) Machine Learning (ML): Machine learning is the scientific study of algorithms and statistical models that computer systems use to effectively perform a specific task without using explicit instructions, relying on patterns and inference instead. It is seen as a subset of artificial intelligence.

(5) “Shall” indicates a mandatory requirement.

(6) “Should” indicates a recommendation or that which is advised but not required.

(7) “Business Continuity” means an ongoing process to ensure that the necessary steps are taken to identify the impact of potential losses and maintain viable recovery strategies, recovery plans, and continuity of services.

(1) "Capital Planning and Investment Control (CPIC)" Capital planning and investment control means the same as capital programming and is a decision-making process for ensuring IT investments integrate strategic planning, budgeting, procurement, and the management of IT in support of agency missions and business needs. The term comes from the Clinger-Cohen Act of 1996 and generally is used in relationship to IT management issues.

(2) "Continuity" includes business continuity, continuity of operations, operational continuity, succession and occupant emergency planning, which support the resilience of the Agency.

(3) "Exercise" means activity in which the Agency's plan(s) is rehearsed in part or in whole to ensure that the plan(s) contains the appropriate information and produces the desired result when put into effect.

(4) "Impact Analysis" or "Business Impact Analysis" or "BIA" means a management level analysis that identifies the impact of losing the Agency's resources.

(5) "Recovery" means activities and programs designed to return conditions to a level that is acceptable to the Agency.

(6) "Response" means immediate and ongoing activities, tasks, programs, and systems to manage the effects of an incident that threatens life, property, operations, or the environment.

(7) "Risk Assessment" means a process of hazard identification, probability analysis, vulnerability analysis, and impacts analysis.

(8) "Service" means and covers Directors of VOA, TSI, OCB; and its own subordinate Directors and Managers of Divisions and Services –to include Grantees

(g) AUTHORIZATION DATE AND APPROVAL:

Approved by: Effective Date:

___________________________________ ________________

CEO and Director