Adaptive AI Risk & Assurance Framework

Assessment Checklist

Prepared For: _____

Prepared By: _____

Date: _____

Section	Function	Purpose
3	Program Management	Overarching governance and management structure.
2.1	Identify	Understanding and managing AI-specific risk.
2.2	Protect	Safeguards to ensure AI system integrity.
2.3	Detect	Detection of AI cybersecurity events.
2.4	Respond	Incident Rating planning and action.
2.5	Recover	Restoration and improvement post-incident.
5.1	Cloud	Cloud-specific AI risk and control measures.
5.2	Embedded	Embedded system-specific risk and controls.

Contents

Instructions for the Assessor:

Purpose: This checklist is designed to assess an organization's adherence to the Adaptive AI Risk & Assurance Framework (AAIRAF) for AI systems deployed in cloud environments and embedded systems, particularly within the context of critical applications like weapon systems, healthcare devices, ICS, etc.
Scope: Prior to starting, clearly define the scope of the assessment (which AI system(s), which lifecycle stages, which environment(s) - cloud, embedded, or hybrid).
Evidence Collection: For each item, record evidence (e.g., policy documents, configuration files, interview notes, test results, logs, screenshots, system architecture diagrams).
Rating:
o **Y (Yes):** The control/practice is fully implemented and effective.
o **N (No):** The control/practice is not implemented.
o **P (Partial):** The control/practice is partially implemented or has deficiencies.
o **NA (Not Applicable):** The control/practice does not apply to the current scope. Provide justification.
o You can also use percentage of one for quantitative risk values (eg. ".2")
Notes/Evidence: Provide detailed comments, observations, and references to evidence.
Maturity Assessment: Use the Maturity Model (Section 4.2 of AAIRAF) to determine the overall maturity level of the organization's AI security posture based on the assessment findings.
AAIRAF ASSESSOR CHECKLIST
Assessor Name:
Date of Assessment:
Organization:
AI System(s) Under Assessment:
Deployment Environment(s): [ ] Cloud [ ] Embedded System [ ] Hybrid [ ] On Premises [ ]

SECTION A: PROGRAM MANAGEMENT & CROSS-CUTTING CAPABILITIES *(Derived from AAIRAF Section 3)*

Ref (AAIRAF)	Checklist Item	Assessor Rating (Y/N/P/NA)	Notes/Evidence
3.1.1	Is there clear leadership and governance for AI security (e.g., dedicated lead/team, integration with CISO)? PS-3, SA-1 • **PS-3(Privacy Planning):** Employ system security and privacy engineering principles in the specification, design, development, implementation, and modification of the system. • The presence of clear leadership and governance for AI security is fundamental to applying security and privacy engineering principles throughout the AI system's lifecycle. Without dedicated leadership, it's unlikely that security and privacy will be adequately considered during planning, design, development, and operations • **SA-1 (System Security and Privacy Policy and Procedures)** is important, it focuses on the existence of documented policies and procedures. The question is probing whether there is leadership and governance to ensure those policies and procedures are followed and effective, not just whether they exist on paper. Having a documented policy without anyone actively championing it is often insufficient.		

Ref (AAIRAF)	Checklist Item	Assessor Rating (Y/N/P/NA)	Notes/Evidence
3.1.2	Are adequate financial, personnel, and technological resources allocated to AI security initiatives? PM-7 • **PM-7 (Enterprise Architecture):** The organization: • (a) Develops and maintains an enterprise architecture that: • (1) Describes the current state of the organization • (2) Describes the target state of the organization • (3) Provides a transition strategy for moving from the current state to the target state; and • (4) Is consistent with applicable laws, directives, regulations, policies, standards, and guidance • (b) Implements a capital planning and investment control process that aligns with the enterprise architecture • (c) Implements the organizational information security architecture throughout the system development life cycle; and • (d) Establishes and maintains baseline configurations and inventories of organizational systems (including hardware, software, firmware, and documentation)		

Ref (AAIRAF)	Checklist Item	Assessor Rating (Y/N/P/NA)	Notes/Evidence
	throughout the system development life cycle.		
3.1.3	Are specific policies and procedures governing secure AI development, deployment, and operation developed and enforced? SA-1 • **SA-1 (System and Services Acquisition Policy and Procedures)** • The organization: • (a) Develops, documents, and disseminates to [Assignment: organization-defined personnel and roles] a system and services acquisition policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and • (b) Develops, documents, and implements procedures to facilitate the implementation of the system and services acquisition policy and associated controls.		
3.2.1	Is due diligence and continuous monitoring performed for third-party AI models, data providers, and tools? SA-9, SI-4 • **SA-9 (External System Services):** (a) Requires that providers of external information system services		

Ref (AAIRAF)	Checklist Item	Assessor Rating (Y/N/P/NA)	Notes/Evidence
	comply with organizational information security requirements and employ security controls commensurate with those requirements • (b) Defines and documents service level agreements with providers of external information system services to ensure that security requirements are met; and • (c) Monitors service provider performance in accordance with service level agreements. • **SI-4 (System Monitoring):** While you might use SI-4 to technically monitor the behavior of a third-party system, this question is about the broader due diligence and monitoring process , not just the technical aspects.		
3.2.2	Do contracts with AI-related third parties include specific security, privacy, and incident Rating requirements? SA-4(2) • **SA-4(2)(Supply Chain Risk Management Plan):** The organization develops, documents, and implements a supply chain risk management plan to address the risks associated with the acquisition of systems and services from external providers.		

Ref (AAIRAF)	Checklist Item	Assessor Rating (Y/N/P/NA)	Notes/Evidence
	• Allocates supply chain protection responsibilities in contracts.		
3.2.3	Are mechanisms in place to verify the provenance and integrity of all AI components from external sources? SR-4, SI-7 • **SR-4(Supply Chain Risk Management Plan):** Requires organizations to establish processes to identify and address weaknesses or deficiencies in the supply chain elements and processes...and to employ controls to protect against supply chain risks... • The question directly addresses the act of verifying the provenance and integrity of AI components from external sources . This falls squarely under the goal of SR-4, which is to secure the supply chain and prevent compromised components from entering your environment • **SI-7 (Software, Firmware, and Information Integrity):** While SI-7 deals with integrity, this question is specifically about how to check for the information to ensure the integrity of the components being added, and not how to confirm the integrity in place.		

Ref (AAIRAF)	Checklist Item	Assessor Rating (Y/N/P/NA)	Notes/Evidence
3.3.1	Is specialized training provided to AI/ML engineers and MLOps teams on secure AI development practices? AT-2, AT-3, PS-3, • **AT-2 (Security Awareness Training):** Provide security awareness training to organizational personnel (including managers, senior executives, and contractors): (i) Before being granted access to the information system; and (ii) Annually thereafter. • **AT-3 (Advanced Training):** Provide advanced security training to privileged users and personnel with security responsibilities • **PS-3 (System Security and Privacy Engineering Principles):** While understanding security principles is helpful, this question is about the delivery of that knowledge through training, not just the existence of the principles.		
3.3.2	Are awareness programs for all employees on AI risks, social engineering, and ethical AI use conducted regularly? AT-2 • **AT-2 (Security Awareness Training):** Provide security awareness training to organizational personnel (including managers, senior executives, and contractors): (i) Before being granted access to the		

Ref (AAIRAF)	Checklist Item	Assessor Rating (Y/N/P/NA)	Notes/Evidence
	information system; and (ii) Annually thereafter.		
3.4.1	Are Key Performance Indicators (KPIs) for AI security effectiveness defined and tracked? MA-1 • **MA-1:** a. Schedule, perform, document, and retain records of maintenance and repairs on the information system in accordance with manufacturer or vendor specifications and organizational policies and procedures; and b. Provide qualified personnel to perform information system maintenance.		
3.4.2	Are Key Risk Indicators (KRIs) for AI-specific risks (e.g., data drift, bias detection) established and monitored? SI-4 • **SI-4:** a. Monitor the system to detect: 1. Attacks and indicators of potential attacks in accordance with the following monitoring objectives: [Assignment: organization-defined monitoring objectives]; and 2. Unauthorized local, network, and remote connections.		
3.4.3	Are regular reporting mechanisms in place to communicate AI security posture and risk		

Ref (AAIRAF)	Checklist Item	Assessor Rating (Y/N/P/NA)	Notes/Evidence
	to leadership? PM-9; Less Direct: SI-4, MA-1, RA-3 • **PM-9:** The organization develops and implements a reporting process that provides the [Assignment: organization-defined frequency and content of information security reports] to [Assignment: organization-defined recipients (i.e., organizational officials)] to obtain awareness of the security state of the organization and the information systems to support [Assignment: organization-defined organizational objectives]. • **Less direct:** • **SI-4 (System Monitoring):** SI-4 focuses on the technical monitoring of the system. This question is about the communication of the information derived from that monitoring to leadership. • **MA-1 (System Maintenance):** Is there a robust procedure to confirm requirements have been met? • **RA-3 (Risk Assessment):** RA-3 deals with assessing risk. This question is about reporting the current risk posture based on ongoing activities.		
3.5.1	Is there an AI Ethics Committee or review board to assess ethical implications and bias in AI projects? PS-3		

Ref (AAIRAF)	Checklist Item	Assessor Rating (Y/N/P/NA)	Notes/Evidence
	• **PS-3 (Privacy Planning):** Employ system security and privacy engineering principles in the specification, design, development, implementation, and modification of the system.		
3.5.2	Is legal counsel involved in the review of AI systems, especially those dealing with sensitive data or high-risk applications? RA-3 • **RA-3 (Risk Assessment):** Assess risks to the organization and individuals, resulting from the operation of the information system, i.e., the potential for loss of confidentiality, integrity, and availability of the system and its information. A key part of this involves identifying controls.		
3.6.1	Are human oversight, intervention, and override mechanisms clearly defined and integrated into AI workflows? PS-3 • **PS-3 (Privacy Planning):** Employ system security and privacy engineering principles in the specification, design, development, implementation, and modification of the system.		

Ref (AAIRAF)	Checklist Item	Assessor Rating (Y/N/P/NA)	Notes/Evidence
3.6.2	Is a clear accountability framework established for decisions and outcomes involving AI systems? SA-1 • **SA-1 (System and Services Acquisition Policy and Procedures):** Develop, document, and disseminate to [Assignment: organization-defined personnel or roles] a system security and privacy policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and procedures to operationalize the policy and associated controls. • The core concept of an "accountability framework" fits perfectly into the scope of a "system security and privacy policy." A good accountability framework involves clearly defining: • **Roles:** Who is responsible for what? • **Responsibilities:** What are the specific duties of each role? • **Decision-Making Processes:** How are decisions made about the AI system? • **Consequences:** What are the potential consequences for failing to meet responsibilities?		

Ref (AAIRAF)	Checklist Item	Assessor Rating (Y/N/P/NA)	Notes/Evidence
3.6.3	Do AI systems log decisions, human interventions, and relevant context to enable post-hoc analysis and auditing? AU-6 • **AU-6 (Audit and Accountability):** a. Review and analyze information system audit records [Assignment: organization-defined frequency] for indications of [Assignment: organization-defined inappropriate or unusual activity]; and b. Report findings to [Assignment: organization-defined personnel or roles].		

SECTION B: CORE FUNCTIONS ASSESSMENT

2.1. IDENTIFY & GOVERN AI RISK (IGR)

2.1.1 AI Asset Management (AI-AM)			
Ref (AAIRAF)	**Checklist Item**	**Assessor Rating (Y/N/P/NA)**	**Notes/Evidence**
2.1.1.1	Is there an up-to-date inventory of all AI systems, models, datasets, libraries, frameworks, and infrastructure? *(Supplemental Guidance: AI RMF Map1.1, AI RMF Govern 1.6, CM-8, RA-2, PL-2, PM-5; MITRE ATLAS Discovery)* • **CM-8 (Configuration Management):** The organization develops, documents,		

2.1.1 AI Asset Management (AI-AM)			
Ref (AAIRAF)	**Checklist Item**	**Assessor Rating (Y/N/P/NA)**	**Notes/Evidence**
	and implements baseline configurations for the information system.		
2.1.1.2	Are AI systems classified based on criticality, potential impact (safety, financial, ethical, mission), and data sensitivity? *(Supplemental Guidance: AI RMF Map1.1, AI RMF Govern 1.6, CM-8, RA-2, PL-2, PM-5; MITRE ATLAS Discovery) PM-7, RA-2* • **PM-7 (Program Management)** The organization allocates [Assignment: organization-defined resources] to adequately protect the information system. • **RA-2 (Risk Assessment)** The organization categorizes the information system and the information contained therein in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidelines.		
2.1.1.3	Is data lineage and provenance for AI training and inference data documented and maintained? *(Supplemental Guidance: AI RMF Map1.1, AI RMF Govern 1.6, CM-8, RA-2, PL-2, PM-5; MITRE ATLAS Discovery)* • **CM-8 (Configuration Management)** Information System Component Inventory: The organization develops,		

2.1.1 AI Asset Management (AI-AM)			
Ref (AAIRAF)	**Checklist Item**	**Assessor Rating (Y/N/P/NA)**	**Notes/Evidence**
	documents, and maintains an inventory of information system components that: A. Accurately reflects the current information system B. Includes all components within the authorization boundary of the information system C. Is at the level of granularity deemed necessary for tracking and reporting; and D. Includes at a minimum [Assignment: Organization-defined information deemed necessary to achieve effective asset management].		
2.1.1.4	Are AI system dependencies (AI Model, hardware, cloud services, third-party models) identified and documented? *(Supplemental Guidance: AI RMF Map1.1, AI RMF Govern 1.6, CM-8, RA-2, PL-2, PM-5; MITRE ATLAS Discovery)* • **CM-8 (Configuration Management)** Information System Component Inventory: The organization develops, documents, and maintains an inventory of information system components that: E. Accurately reflects the current information system F. Includes all components within the authorization boundary of the information system		

2.1.1 AI Asset Management (AI-AM)			
Ref (AAIRAF)	**Checklist Item**	**Assessor Rating (Y/N/P/NA)**	**Notes/Evidence**
	G. Is at the level of granularity deemed necessary for tracking and reporting; and Includes at a minimum [Assignment: Organization-defined information deemed necessary to achieve effective asset management].		
2.1.2 AI Governance & Risk Management Strategy (AI-GRS)			
2.1.2.1	Are formal policies for managing AI-specific cybersecurity, privacy, and ethical risks established and integrated with enterprise risk management? PM-1 • **PM-1 (Program Management) :** The organization manages the information security program including developing and issuing security policies		
2.1.2.2	Are roles, responsibilities, and accountability for AI risk management clearly defined (e.g., AI Ethics Board, MLSecOps)? SA-1 • **SA-1 (System and Services Acquisition):** Requires the organization to develop, document, and disseminate a system security and privacy policy that addresses roles, responsibilities, and accountability .		

2.1.1 AI Asset Management (AI-AM)			
Ref (AAIRAF)	**Checklist Item**	**Assessor Rating (Y/N/P/NA)**	**Notes/Evidence**
2.1.2.3	Are AI risk tolerance and acceptance criteria defined for different categories of AI systems? RA-3 • **RA-3 (Risk Assessment) :** Requires the organization to assess risks to the organization and individuals, resulting from the operation of the information system .		
2.1.2.4	Is there a defined AI supply chain risk management strategy for models, data providers, and third-party AI services? SR-2 • **SR-2 (Supply Chain Risk Management):** The organization develops and implements a plan for managing supply chain risks associated with the research and development, design, manufacturing, acquisition, delivery, integration, operations and maintenance, and disposal of the following systems, system components or system services: [Assignment: organization-defined systems, system components, or system services]		
2.1.3 AI Threat & Vulnerability Assessment (AI-TVA)			
2.1.3.1	Are AI-specific threats (e.g., data poisoning, model evasion, prompt injection) identified and documented (e.g., using MITRE ATLAS)? RA-3		

2.1.1 AI Asset Management (AI-AM)			
Ref (AAIRAF)	**Checklist Item**	**Assessor Rating (Y/N/P/NA)**	**Notes/Evidence**
	• **RA-3 (Risk Assessment) :** Assess risks to the organization and individuals, resulting from the operation of the information system, i.e., the potential for loss of confidentiality, integrity, and availability of the system and its information.		
2.1.3.2	Is adversarial risk profiling performed for AI systems, considering attacker capabilities and motivations? RA-3 • **RA-3: (Risk Assessment) :** Assess risks to the organization and individuals, resulting from the operation of the information system, i.e., the potential for loss of confidentiality, integrity, and availability of the system and its information.		
2.1.3.3	Are vulnerabilities in AI pipelines (MLOps), model architecture, and data processing regularly assessed? SI-2 • **SI-2 (System and Information Integrity):** a. Identify, report, and correct system flaws; b. Test software and firmware updates related to flaw remediation for effectiveness and potential side effects before installation; c. Install security-relevant software and firmware updates within [Assignment: organization-defined time period] of the		

2.1.1 AI Asset Management (AI-AM)			
Ref (AAIRAF)	**Checklist Item**	**Assessor Rating (Y/N/P/NA)**	**Notes/Evidence**
	release of the updates; and d. Incorporate flaw remediation into the organizational configuration management process.		
2.1.3.4	Is AI-specific penetration testing and red-teaming conducted to identify weaknesses? SA-8 • **SA-8 (System and Services Acquisition)** The organization conducts assessments of the security and privacy controls employed within the information system to determine if the controls are effective in accordance with assessment procedures defined in the security and privacy plans.		
2.1.4 AI Regulatory & Ethical Compliance (AI-REC)			
2.1.4.1	Is there a process to identify and comply with AI-specific regulations (e.g., EU AI Act, DoD AI Policies)? SA-1 • **SA-1 (System and Services Acquisition):** Develop, document, and disseminate to [Assignment: organization-defined personnel or roles] a system security and privacy policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance;		

2.1.1 AI Asset Management (AI-AM)			
Ref (AAIRAF)	**Checklist Item**	**Assessor Rating (Y/N/P/NA)**	**Notes/Evidence**
	and procedures to operationalize the policy and associated controls.		
2.1.4.2	Are methodologies in place to assess and mitigate algorithmic bias and fairness concerns? PS-3 • **PS-3 (Personnel Security):** Employ system security and privacy engineering principles in the specification, design, development, implementation, and modification of the system.		
2.1.4.3	Is compliance with data privacy regulations (e.g., GDPR, CCPA) for all AI data ensured? SA-1 • **SA-1 (System and Services Acquisition):** Develop, document, and disseminate to [Assignment: organization-defined personnel or roles] a system security and privacy policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and procedures to operationalize the policy and associated controls.		
2.1.4.4	Are mechanisms established for human oversight, intervention, and accountability in AI decision-making? PS-3		

2.1.1 AI Asset Management (AI-AM)			
Ref (AAIRAF)	**Checklist Item**	**Assessor Rating (Y/N/P/NA)**	**Notes/Evidence**
	• **PS-3 (Personnel Security):** Employ system security and privacy engineering principles in the specification, design, development, implementation, and modification of the system.		

2.2. PROTECT AI ASSETS (PAA)

Ref (AAIRAF)	Checklist Item	Assessor Rating (Y/N/P/NA)	Notes/Evidence
2.2.1 Secure AI Data Management (S-AIDM)			
2.2.1.1	Are secure protocols (e.g., encrypted channels, API validation) used for data collection and ingestion to prevent data poisoning? SC-8 • **SC-8 (System and Communications Protection):** Requires organizations to protect the confidentiality and integrity of transmitted information. The question specifically addresses data poisoning , which is an integrity threat, and ensuring secure protocols for data collection, so they will be protected in transit.		
2.2.1.2	Are privacy-enhancing technologies (PETs) like anonymization, differential privacy, or homomorphic encryption applied where appropriate? PS-3		

Ref (AAIRAF)	Checklist Item	Assessor Rating (Y/N/P/NA)	Notes/Evidence
	• **PS-3 (Personnel Security)*:*** *Employ system security and privacy engineering principles in the specification, design, development, implementation, and modification of the system.*		
2.2.1.3	Are robust data integrity controls (validation, checksums, hashing) implemented for training and production data? SI-7 • **SI-7 (System and Information Integrity):** *Requires organizations to employ integrity verification tools to detect unauthorized changes to the following software, firmware, and information: [Assignment: organization-defined software, firmware, and information]*		
2.2.1.4	Are strict access controls (least privilege, RBAC) and encryption at rest applied for all AI-related datasets? SC-8, AC-3 • **SC-8 (System and Communications Protection):** The organization protects the [Selection (one or more): confidentiality; integrity] of transmitted information. • **AC-3(Access Control):** The organization enforces approved authorizations for logical access to the information system in accordance with applicable policy.		
2.2.2 Secure AI Model Development & Deployment (S-AIMDD)			

Ref (AAIRAF)	Checklist Item	Assessor Rating (Y/N/P/NA)	Notes/Evidence
2.2.2.1	Are security controls implemented across the MLOps pipeline, including secure CI/CD and vulnerability scanning of container images? CM-6 • **CM-6 (Configuration Management):** Requires the organization to manage and control configuration settings for information technology products employed within the information system using secure configuration settings		
2.2.2.2	Are adversarial robustness techniques (e.g., adversarial training, input sanitization) incorporated into model development? PS-3 • **PS-3 (Personnel Security):** Requires the organization to employ system security and privacy engineering principles in the specification, design, development, implementation, and modification of the system .		
2.2.2.3	Is model integrity verification (digital signatures, checksums) implemented to detect unauthorized modifications? SI-7 • **SI-7 (System and Information Integrity):** Requires organizations to employ integrity verification tools to detect unauthorized changes to defined software, firmware, and information.		
2.2.2.4	Are model inference endpoints secured with authentication, authorization, rate limiting, and input validation? AC-3, SC-5, SI-10		

Ref (AAIRAF)	Checklist Item	Assessor Rating (Y/N/P/NA)	Notes/Evidence
	• **AC-3 – (Access Enforcement)** The organization enforces approved authorizations for logical access to the information system in accordance with applicable policy [Access Control Policy & Procedures]. • **SC-5 (System and Communications Protection)- Denial-of-Service Protection** a. [Selection (one): Protect against; Limit] the effects of the following types of denial-of-service events: [Assignment: organization-defined types of denial-of-service events]; and b. Employ the following controls to achieve the denial-of-service objective: [Assignment: organization-defined controls by type of denial-of-service event]. • **SI-10 (System and Information Integrity) - Input Validation** The organization checks the validity of [Assignment: organization-defined information inputs to the system].		
2.2.2.5	Is secure configuration management maintained for all AI development and production environments? CM-6 • **CM-6 (Configuration Management):** Requires the organization to manage and control configuration settings for information technology products employed within the information system using secure configuration settings .		

Ref (AAIRAF)	Checklist Item	Assessor Rating (Y/N/P/NA)	Notes/Evidence
	• This directly addresses the need for properly secured environments for data to prevent potential exposure.		
2.2.3 AI Access Control & Authorization (AI-ACA)			
2.2.3.1	Is strong authentication and granular authorization implemented for access to AI development environments, data lakes, and inference services? AC-3, IA-5 • **AC-3 (Access Control) - Access Enforcement** The organization enforces approved authorizations for logical access to the information system in accordance with applicable policy [Access Control Policy & Procedures]. • **IA-5 (Identification and Authentication)-Authenticator Management** The organization manages information system authenticators (e.g., passwords, tokens, biometrics)		
2.2.3.2	Are interfaces for human oversight and intervention (human-in-the-loop) secure and validated? PS-3 • **PS-3 (Personnel Security):** Employ system security and privacy engineering principles in the specification, design, development, implementation, and modification of the system.		
2.2.4 AI System Resilience & Redundancy (AI-SRR)			

Ref (AAIRAF)	Checklist Item	Assessor Rating (Y/N/P/NA)	Notes/Evidence
2.2.4.1	Are backup and recovery strategies defined and tested for AI models, training data, and infrastructure? CP-9 • **CP-9 (Contingency Planning):** The organization implements and maintains a recovery plan for organizational information systems to ensure timely restoration of essential capabilities following a disruption.		
2.2.4.2	Is high availability ensured for critical AI services through redundancy and failover mechanisms? CP-9 • **CP-9(Contingency Planning):** The organization implements and maintains a recovery plan for organizational information systems to ensure timely restoration of essential capabilities following a disruption.		
2.2.4.3	Is contingency planning developed and tested for AI system failures or attacks? CP-9 • **CP-9 (Contingency Planning):** The organization implements and maintains a recovery plan for organizational information systems to ensure timely restoration of essential capabilities following a disruption.		
2.2.5 AI Explainability & Interpretability Controls (AI-EIC)			
2.2.5.1	Are explainable AI (XAI) techniques implemented appropriate to provide insights into model decisions? PS-3		

Ref (AAIRAF)	Checklist Item	Assessor Rating (Y/N/P/NA)	Notes/Evidence
	• **PS-3 (Personnel Security):** Requires organizations to employ security and privacy principles to ensure systems are implemented in a secure fashion. • Implementing XAI techniques to provide insights relies on understanding models and various potential data biases to meet security goals.		
2.2.5.2	Is comprehensive documentation of model architecture, training parameters, and version history maintained? CM-8 • **CM-8 (Configuration Management):** The organization develops documents and maintains an inventory of information system components.		
2.2.5.3	Are robust logging and audit trails implemented for AI system inputs, outputs, and internal decision-making processes? AU-6 • **AU-6 (Audit and Accountability)** The organization: • a. Reviews and analyzes information system audit records [Assignment: organization-defined frequency] for indications of [Assignment: organization-defined inappropriate or unusual activity]; and • b. Reports findings to [Assignment: organization-defined personnel or roles].		

2.3. DETECT AI INCIDENTS (DAI)

Ref (AAIRAF)	Checklist Item	Assessor Rating (Y/N/P/NA)	Notes/Evidence
2.3.1 AI Anomaly & Threat Detection (AI-ATD)			
2.3.1.1	Is monitoring in place for adversarial attacks (e.g., unusual input patterns, sudden performance drops)? SI-4 • **SI-4 (System and Information Integrity)** The organization: • a. Monitors the system to detect: • Attacks and indicators of potential attacks in accordance with the following monitoring objectives: [Assignment: organization-defined monitoring objectives]; and • Unauthorized local, network, and remote connections;		
2.3.1.2	Is data drift, concept drift, and model decay continuously detected? SI-4 • **SI-4 (System and Information Integrity)**The organization: • a. Monitors the system to detect: Attacks and indicators of potential attacks in accordance with the following monitoring objectives: [Assignment: organization-defined monitoring objectives]; and unauthorized local, network, and remote connections • b. Identifies unauthorized use of the system through the following techniques and methods: [Assignment: organization-defined techniques and methods] • c. Invokes internal monitoring capabilities or deploy monitoring devices: Strategically within the system to collect organization-determined		

Ref (AAIRAF)	Checklist Item	Assessor Rating (Y/N/P/NA)	Notes/Evidence
	essential information; and At ad hoc locations within the system to track specific types of transactions of interest to the organization		
2.3.1.3	Is model tampering and integrity continuously monitored (e.g., via cryptographic hashes or behavioral baselines)? SI-7 • **SI-7 (System and Information Integrity)** The organization: • a. Employs integrity verification tools to detect unauthorized changes to the following software, firmware, and information: [Assignment: organization-defined software, firmware, and information]; and • b. Takes the following actions when unauthorized changes to the software, firmware, and information are detected: [Assignment: organization-defined actions].		
2.3.1.4	Are AI system logs and telemetry analyzed for suspicious activity? SI-4 • **SI-4 (System and Information Integrity):** The organization: • Monitors the system to detect: • Attacks and indicators of potential attacks in accordance with the following monitoring objectives: [Assignment: organization-defined monitoring objectives]; and unauthorized local, network, and remote connections; Identifies unauthorized use of the system through the following techniques and methods: [Assignment: organization-defined techniques and methods];		

Ref (AAIRAF)	Checklist Item	Assessor Rating (Y/N/P/NA)	Notes/Evidence
	Invokes internal monitoring capabilities or deploy monitoring devices: • Strategically within the system to collect organization-determined essential information; and At ad hoc locations within the system to track specific types of transactions of interest to the organization; Analyzes detected events and anomalies; Adjusts the level of system monitoring activity when there is a change in risk to organizational operations and assets, individuals, other organizations, or the Nation • Obtains legal opinion regarding system monitoring activities; and provides [Assignment: organization-defined system monitoring information] to [Assignment: organization-defined personnel or roles] [Selection (one or more): as needed; [Assignment: organization-defined frequency]].		
2.3.2 AI Performance & Bias Monitoring (AI-PBM)			
2.3.2.1	Are key model performance metrics (accuracy, precision, recall) continuously monitored in real-time? SI-4 • **SI-4 (System and Information Integrity):** The organization: Monitors the system to detect: Attacks and indicators of potential attacks in accordance with the following monitoring objectives: [Assignment: organization-defined monitoring objectives]; and unauthorized local, network, and remote connections		

Ref (AAIRAF)	Checklist Item	Assessor Rating (Y/N/P/NA)	Notes/Evidence
	• Identifies unauthorized use of the system through the following techniques and methods: [Assignment: organization-defined techniques and methods • Invokes internal monitoring capabilities or deploy monitoring devices: • Strategically within the system to collect organization-determined essential information; and at ad hoc locations within the system to track specific types of transactions of interest to the organization • Analyzes detected events and anomalies; Adjusts the level of system monitoring activity when there is a change in risk to organizational operations and assets, individuals, other organizations, or the Nation • Obtains legal opinion regarding system monitoring activities; and Provides [Assignment: organization-defined system monitoring information] to [Assignment: organization-defined personnel or roles] [Selection (one or more): as needed; [Assignment: organization-defined frequency]].		
2.3.2.2	Is algorithmic bias continuously monitored for shifts or unfair outcomes? SI-4 The organization: • **SI-4 (System and Information Integrity)**Monitors the system to detect: 1. Attacks and indicators of potential attacks in accordance with the following monitoring		

Ref (AAIRAF)	Checklist Item	Assessor Rating (Y/N/P/NA)	Notes/Evidence
	objectives: [Assignment: organization-defined monitoring objectives]; and unauthorized local, network, and remote connections • Identifies unauthorized use of the system through the following techniques and methods: [Assignment: organization-defined techniques and methods] Invokes internal monitoring capabilities or deploy monitoring devices: • Strategically within the system to collect organization-determined essential information; and at ad hoc locations within the system to track specific types of transactions of interest to the organization • Analyzing detected events and anomalies adjusts the level of system monitoring activity when there is a change in risk to organizational operations and assets, individuals, other organizations, or the Nation • Obtains legal opinion regarding system monitoring activities; and provides [Assignment: organization-defined system monitoring information] to [Assignment: organization-defined personnel or roles] [Selection (one or more): as needed; [Assignment: organization-defined frequency]].		
2.3.2.3	Are automated checks on AI system outputs implemented to identify anomalous or nonsensical predictions? SI-4 • **SI-4 (System and Information Integrity)**The organization:		

Ref (AAIRAF)	Checklist Item	Assessor Rating (Y/N/P/NA)	Notes/Evidence
	• Monitors the system to detect: Attacks and indicators of potential attacks in accordance with the following monitoring objectives: [Assignment: organization-defined monitoring objectives]; and unauthorized local, network, and remote connections • Identifies unauthorized use of the system through the following techniques and methods: [Assignment: organization-defined techniques and methods] • Invokes internal monitoring capabilities or deploy monitoring devices: Strategically within the system to collect organization-determined essential information; and At ad hoc locations within the system to track specific types of transactions of interest to the organization • Analyzes detected events and anomalies; Adjusts the level of system monitoring activity when there is a change in risk to organizational operations and assets, individuals, other organizations, or the Nation • Obtains legal opinion regarding system monitoring activities; and Provides [Assignment: organization-defined system monitoring information] to [Assignment: organization-defined personnel or roles] [Selection (one or more): as needed; [Assignment: organization-defined frequency]].		
2.3.3 AI Security Continuous Monitoring (AI-SCM)			
2.3.3.1	Is continuous vulnerability scanning performed for AI-related infrastructure and dependencies? SI-2		

Ref (AAIRAF)	Checklist Item	Assessor Rating (Y/N/P/NA)	Notes/Evidence
	• **SI-2 (System and Information Integrity)** The organization: • a. Identifies, reports, and corrects information system flaws in a timely manner • b. Tests software and firmware updates related to flaw remediation for effectiveness and potential side effects before installation • c. Installs security-relevant software and firmware updates within [Assignment: organization-defined time] of the release of the updates; and • d. Incorporates flaw remediation into the organizational configuration management process.		
2.3.3.2	Are external threat intelligence sources for new AI attack techniques integrated into security operations? SI-4 • **SI-4 (System and Information Integrity)** The organization: • Monitors the system to detect: Attacks and indicators of potential attacks in accordance with the following monitoring objectives: [Assignment: organization-defined monitoring objectives]; and unauthorized local, network, and remote connections • Identifies unauthorized use of the system through the following techniques and methods: [Assignment: organization-defined techniques and methods] • Invokes internal monitoring capabilities or deploy monitoring devices: Strategically within the system to collect organization-determined essential information; and At ad hoc locations		

Ref (AAIRAF)	Checklist Item	Assessor Rating (Y/N/P/NA)	Notes/Evidence
	within the system to track specific types of transactions of interest to the organization • Analyzes detected events and anomalies; Adjusts the level of system monitoring activity when there is a change in risk to organizational operations and assets, individuals, other organizations, or the Nation • Obtains legal opinion regarding system monitoring activities; and Provides [Assignment: organization-defined system monitoring information] to [Assignment: organization-defined personnel or roles] [Selection (one or more): as needed; [Assignment: organization-defined frequency]].		
2.3.3.3	Are automated checks performed for secure configuration of AI environments against baselines? CM-6 • **CM-6 (Configuration Management):** The organization: • Establishes and documents configuration settings for information technology products employed within the information system using [Selection: security configuration checklists; benchmarks; [Assignment: organization-defined configuration guidelines] that: • Reflect the intent of the security and privacy requirements outlined in applicable laws, Executive Orders, directives, regulations, policies, standards, and guidelines • Are consistent with manufacturer- or developer-provided security guidance		

Ref (AAIRAF)	Checklist Item	Assessor Rating (Y/N/P/NA)	Notes/Evidence
	• Consider the complete system, the intended system operational environment, and organization-defined non-security requirements; and • Are reviewed and updated [Assignment: organization-defined frequency]; and • Implements the configuration settings.		

2.4. RESPOND TO AI INCIDENTS (RAI)

Ref (AAIRAF)	Checklist Item	Assessor Rating (Y/N/P/NA)	Notes/Evidence
2.4.1 AI Incident Rating Planning (AI-IRP)			
2.4.1.1	Are AI-specific incident Rating plans (e.g., for data poisoning, model theft, adversarial attacks) developed and regularly tested? IR-2 • **IR-2 (Incident Response) - Incident Response Training** • The organization provides incident response training to information system users and personnel with assigned roles and responsibilities in accordance with applicable policies and procedures.		
2.4.1.2	Are roles and responsibilities for AI incident Rating teams defined? IR-4 • **IR-4 (Incident Response)- Incident Handling** • The organization:		

Ref (AAIRAF)	Checklist Item	Assessor Rating (Y/N/P/NA)	Notes/Evidence
	o Implements a process for: • Detecting information system security incidents. • Analyzing information system security incidents to determine the nature of the incidents. • Prioritizing incident handling activities. • Documenting information system security incidents; and • Reporting information system security incidents to [Assignment: organization-defined personnel and/or roles] in accordance with applicable reporting requirements. o Employs automated mechanisms to support incident handling; and o Provides a defined Contact to third party vendors to maintain compliancy.		
2.4.1.3	Are communication protocols for AI incidents (internal, external, regulatory) established? IR-4 • **IR-4 (Incident Response) - Incident Handling** • The organization: o Implements a process for: • Detecting information system security incidents. • Analyzing information system security incidents to determine the nature of the incidents. • Prioritizing incident handling activities. • Documenting information system security incidents; and		

Ref (AAIRAF)	Checklist Item	Assessor Rating (Y/N/P/NA)	Notes/Evidence

	• Reporting information system security incidents to [Assignment: organization-defined personnel and/or roles] in accordance with applicable reporting requirements.
	  o Employs automated mechanisms to support incident handling; and
	  o Provides a defined Contact to third party vendors to maintain compliancy.		

2.4.2 AI Incident Containment & Eradication (AI-ICE)			
2.4.2.1	Are strategies in place for isolating compromised AI models or data pipelines? IR-5 • **IR-5 (Incident Response)- Incident Containment** • The organization contains information system security incidents.		
2.4.2.2	Are methods defined for removing poisoned data or compromised model versions? IR-5 • **IR-5 (Incident Response)- Incident Containment** • The organization contains information system security incidents.		
2.4.2.3	Are procedures in place for rolling back to a secure, pre-attack model state? CP-9 • **CP-9 (Contingency Planning)- Information System Backup, Recovery, and Reconstitution** • The organization:		

Ref (AAIRAF)	Checklist Item	Assessor Rating (Y/N/P/NA)	Notes/Evidence
	○ Performs and documents testing and exercises of the information system contingency plan that: • Include [Selection (one or more): hostile cyber-attack scenarios; [Assignment: organization-defined operational events or conditions] • Establish and test the effectiveness of: • Backup information system processing and storage capabilities; and • Recovery and reconstitution procedures; and • Identify and address lessons learned from the testing and exercise activities • Coordinates contingency planning, testing, and exercise activities with [Assignment: organization-defined organizational entities]; and • Reviews and updates the contingency plan [Assignment: organization-defined frequency] and following testing/exercise activities.		
2.4.3 AI Incident Analysis & Forensics (AI-IAF)			
2.4.3.1	Is collection and analysis of AI-specific forensic artifacts (e.g., model weights, training logs) performed? SI-4; (less direct = **IR-3, IR-5, CP-9)** • **SI-4 (System and Information Integrity) - System Monitoring** • The organization: • Monitors the system to detect: • Attacks and indicators of potential attacks in accordance with the following monitoring		

Ref (AAIRAF)	Checklist Item	Assessor Rating (Y/N/P/NA)	Notes/Evidence
	objectives: [Assignment: organization-defined monitoring objectives]; and • Unauthorized local, network, and remote connections • Identifies unauthorized use of the system through the following techniques and methods: [Assignment: organization-defined techniques and methods] • Invokes internal monitoring capabilities or deploy monitoring devices: • Strategically within the system to collect organization-determined essential information; and • At ad hoc locations within the system to track specific types of transactions of interest to the organization • Analyzes detected events and anomalies • Adjusts the level of system monitoring activity when there is a change in risk to organizational operations and assets, individuals, other organizations, or the Nation • Obtains legal opinion regarding system monitoring activities; and • Provides [Assignment: organization-defined system monitoring information] to [Assignment: organization-defined personnel or roles] [Selection (one or more): as needed; [Assignment: organization-defined frequency]]. • **IR-3 (Incident Response) Incident Response Training**		

Ref (AAIRAF)	Checklist Item	Assessor Rating (Y/N/P/NA)	Notes/Evidence
	• (a) Provide incident response training to organizational personnel: • (1) Consistent with assigned roles and responsibilities • (2) Within [Assignment: organization-defined time period] of assuming an incident response role; and • (3) At least [Assignment: organization-defined frequency] thereafter. • (b) Incorporate simulated events into incident response training to facilitate effective response by personnel. • **IR-5 (Incident Response) Incident Monitoring** • The organization: • (a) Monitors security alerts and advisories regarding organizational systems and information • (b) Coordinates incident monitoring activities with [Assignment: organization-defined entities] • (c) Establishes contact with [Assignment: organization-defined entities] to facilitate the sharing of information regarding alerts and advisories • (d) Implements [Assignment: organization-defined procedures] for the receipt, analysis, and dissemination of security alerts and advisories; and • (e) Disseminates security alerts and advisories to [Assignment: organization-defined personnel and roles]. • **CP-9 (Contingency Planning) System Backup and Recovery** • The organization: • (a) Conducts backups of [Assignment: organization-defined information system] [Selection: daily; weekly; monthly] • (b) Develops, documents, and periodically tests procedures for the recovery of organizational systems to support essential mission/business functions in the event of a system failure		

Ref (AAIRAF)	Checklist Item	Assessor Rating (Y/N/P/NA)	Notes/Evidence
	• (c) Protects the confidentiality, integrity, and availability of backup information at storage locations; and • (d) Conducts backups of critical information system software and information.		

2.4.3.2	Is root cause analysis performed for AI incidents (e.g., identifying source of adversarial input)? IR-4
	• **IR-4 (Incident Response) - Incident Handling**
	• The organization:
	  o Implements a process for:
	• Detecting information system security incidents.
	• Analyzing information system security incidents to determine the nature of the incidents.
	• Prioritizing incident handling activities.
	• Documenting information system security incidents; and
	• Reporting information system security incidents to [Assignment: organization-defined personnel and/or roles] in accordance with applicable reporting requirements.
	  o Employs automated mechanisms to support incident handling; and
	  o Provides a defined Contact to third party vendors to maintain compliancy.		

2.4.3.3	Is explainability analysis of anomalous AI behavior used during an incident? IR-4 • **IR-4 (Incident Response) - Incident Handling** • The organization:		

Ref (AAIRAF)	Checklist Item	Assessor Rating (Y/N/P/NA)	Notes/Evidence
	○ Implements a process for: • Detecting information system security incidents. • Analyzing information system security incidents to determine the nature of the incidents. • Prioritizing incident handling activities. • Documenting information system security incidents; and • Reporting information system security incidents to [Assignment: organization-defined personnel and/or roles] in accordance with applicable reporting requirements. ○ Employs automated mechanisms to support incident handling; and ○ Provides a defined Contact to third party vendors to maintain compliancy.		
2.4.4 AI Remediation & Recovery Coordination (AI-RRC)			
2.4.4.1	Are procedures for retraining models with clean data defined and implemented? CP-9 • **CP-9 (Contingency Planning) - Information System Backup, Recovery, and Reconstitution** • The organization: ○ Performs and documents testing and exercises of the information system contingency plan that: • Include [Selection (one or more): hostile cyber-attack scenarios; [Assignment: organization-defined operational events or conditions]		

Ref (AAIRAF)	Checklist Item	Assessor Rating (Y/N/P/NA)	Notes/Evidence

	• Establish and test the effectiveness of:
	  o Backup information system processing and storage capabilities; and
	  o Recovery and reconstitution procedures; and
	• Identify and address lessons learned from the testing and exercise activities
	  o Coordinates contingency planning, testing, and exercise activities with [Assignment: organization-defined organizational entities]; and
	  o Reviews and updates the contingency plan [Assignment: organization-defined frequency] and following testing/exercise activities.		

2.4.4.2	Are model parameters or architectures updated to mitigate vulnerabilities identified during an incident? SI-2
	• **SI-2 (System and Information Integrity) - Flaw Remediation**
	• The organization:
	  o Identifies, reports, and corrects information system flaws in a timely manner.
	  o Tests software and firmware updates related to flaw remediation for effectiveness and potential side effects before installation.
	• Installs security-relevant software and firmware updates within [Assignment: organization-defined time] of the release of the updates; and		

Ref (AAIRAF)	Checklist Item	Assessor Rating (Y/N/P/NA)	Notes/Evidence
	• Incorporates flaw remediation into the organizational configuration management process.		

2.4.4.3	Is re-deployment of AI systems validated and secured? CM-6
	• **CM-6 (Configuration Management) - Configuration Settings**
	• The organization:
	  o Establishes and documents configuration settings for information technology products employed within the information system using [Selection: security configuration checklists; benchmarks; [Assignment: organization-defined configuration guidelines] that:
	• Reflect the intent of the security and privacy requirements outlined in applicable laws, Executive Orders, directives, regulations, policies, standards, and guidelines
	• Are consistent with manufacturer- or developer-provided security guidance
	• Consider the complete system, the intended system operational environment, and organization-defined non-security requirements; and
	• Are reviewed and updated [Assignment: organization-defined frequency]; and
	  o Implements the configuration settings.		

2.5. RECOVER & EVOLVE AI SYSTEMS (REA)

Ref (AAIRAF)	Checklist Item	Assessor Rating (Y/N/P/NA)	Notes/Evidence
2.5.1 AI Recovery Planning & Implementation (AI-RPI)			
2.5.1.1	Are comprehensive plans for full recovery of AI systems post-incident in place and tested? CP-9 • **CP-9 (Contingency Planning) - Information System Backup, Recovery, and Reconstitution** • The organization: o Performs and documents testing and exercises of the information system contingency plan that: • Include [Selection (one or more): hostile cyber-attack scenarios; [Assignment: organization-defined operational events or conditions] • Establish and test the effectiveness of: • Backup information system processing and storage capabilities; and • Recovery and reconstitution procedures; and • Identify and address lessons learned from the testing and exercise activities. • Coordinates contingency planning, testing, and exercise activities with [Assignment: organization-defined organizational entities]; and • Reviews and updates the contingency plan [Assignment: organization-defined frequency] and following testing/exercise activities.		

Ref (AAIRAF)	Checklist Item	Assessor Rating (Y/N/P/NA)	Notes/Evidence
2.5.1.2	Is validation and testing of recovered AI models and data pipelines performed? CP-9 • **CP-9 (Contingency Planning) - Information System Backup, Recovery, and Reconstitution** • The organization: o Performs and documents testing and exercises of the information system contingency plan that: • Include [Selection (one or more): hostile cyber-attack scenarios; [Assignment: organization-defined operational events or conditions] • Establish and test the effectiveness of: • Backup information system processing and storage capabilities; and • Recovery and reconstitution procedures; and • Identify and address lessons learned from the testing and exercise activities. • Coordinates contingency planning, testing, and exercise activities with [Assignment: organization-defined organizational entities]; and • Reviews and updates the contingency plan [Assignment: organization-defined frequency] and following testing/exercise activities.		
2.5.1.3	Is restoration of data integrity and model trustworthiness ensured post-recovery? CP-9		

Ref (AAIRAF)	Checklist Item	Assessor Rating (Y/N/P/NA)	Notes/Evidence
	• **CP-9 (Contingency Planning) - Information System Backup, Recovery, and Reconstitution** • The organization: o Performs and documents testing and exercises of the information system contingency plan that: • Include [Selection (one or more): hostile cyber-attack scenarios; [Assignment: organization-defined operational events or conditions]] • Establish and test the effectiveness of: • Backup information system processing and storage capabilities; and • Recovery and reconstitution procedures; and • Identify and address lessons learned from the testing and exercise activities. • Coordinates contingency planning, testing, and exercise activities with [Assignment: organization-defined organizational entities]; and • Reviews and updates the contingency plan [Assignment: organization-defined frequency] and following testing/exercise activities.		
2.5.2 AI Communications (AI-COM)			
2.5.2.1	Is communication with stakeholders about AI service restoration and lessons learned managed effectively? IR-4		

Ref (AAIRAF)	Checklist Item	Assessor Rating (Y/N/P/NA)	Notes/Evidence

	• **IR-4 (Incident Response)- Incident Handling**
	• The organization:
	  o Implements a process for:
	• Detecting information system security incidents.
	• Analyzing information system security incidents to determine the nature of the incidents.
	• Prioritizing incident handling activities.
	• Documenting information system security incidents; and
	• Reporting information system security incidents to [Assignment: organization-defined personnel and/or roles] in accordance with applicable reporting requirements.
	  o Employs automated mechanisms to support incident handling; and
	  o Provides a defined Contact to third party vendors to maintain compliancy.		

2.5.2.2	Is transparency with affected parties regarding AI incidents handled according to legal/ethical obligations? IR-4 • **IR-4 (Incident Response)- Incident Handling** • The organization: o Implements a process for:		

Ref (AAIRAF)	Checklist Item	Assessor Rating (Y/N/P/NA)	Notes/Evidence
	1. Detecting information system security incidents. • Analyzing information system security incidents to determine the nature of the incidents. • Prioritizing incident handling activities. • Documenting information system security incidents; and • Reporting information system security incidents to [Assignment: organization-defined personnel and/or roles] in accordance with applicable reporting requirements. • b. Employs automated mechanisms to support incident handling; and • c. Provides a defined Contact to third party vendors to maintain compliancy.		
2.5.3 AI Post-Incident Review & Improvement (AI-PIRI)			
2.5.3.1	Are post-incident reviews conducted to identify lessons learned specific to AI incidents? IR-4 • **IR-4 (Incident Response)- Incident Handling** • The organization: ○ Implements a process for: • Detecting information system security incidents.		

Ref (AAIRAF)	Checklist Item	Assessor Rating (Y/N/P/NA)	Notes/Evidence
	• Analyzing information system security incidents to determine the nature of the incidents. • Prioritizing incident handling activities. • Documenting information system security incidents; and • Reporting information system security incidents to [Assignment: organization-defined personnel and/or roles] in accordance with applicable reporting requirements. • Employs automated mechanisms to support incident handling; and • Provides a defined Contact to third party vendors to maintain compliancy.		
2.5.3.2	Are AI risk assessments and security controls updated based on incident findings and emerging threat intelligence? RA-3 • **RA-3 (Risk Assessment) - Risk Assessment** • The organization: o conducts a risk assessment of the information system [Assignment: organization-defined frequency] o Document the risk assessment results in a risk assessment report o Develops and implements a risk mitigation strategy; and o Reviews and updates the risk assessment [Assignment: organization-defined frequency] or		

Ref (AAIRAF)	Checklist Item	Assessor Rating (Y/N/P/NA)	Notes/Evidence
	whenever there are significant changes to the information system or environment of operation (e.g., new systems, applications, ports, protocols, services, or a change in the threat).		
2.5.3.3	Are continuous training and awareness programs focused on emerging AI threats provided? AT-2 • **AT-2 (Awareness and Training) - Security Awareness Training** • The organization provides security awareness training to information system users (including managers, senior executives, and contractors): o Before being granted access to the information system; and o Annually thereafter.		

SECTION C: ENVIRONMENT-SPECIFIC CONSIDERATIONS

C.1. CLOUD ENVIRONMENT SPECIFIC CHECKS *(Only applicable if AI system is in a Cloud Environment)*

Ref (AAIRAF)	Checklist Item	Assessor Rating (Y/N/P/NA)	Notes/Evidence
5.1	Is the cloud provider's security posture assessed and documented (e.g., SOC 2, ISO 27001 compliance)? SA-9		

Ref (AAIRAF)	Checklist Item	Assessor Rating (Y/N/P/NA)	Notes/Evidence
	• **SA-9 (System and Services Acquisition) - External System Services** o Requires that providers of external system services comply with organizational security requirements and employ the following controls: [Assignment: organization-defined controls]; b. Defines and documents organizational oversight and user roles and responsibilities with regard to external system services; and c. Employs the following processes, methods, and techniques to monitor control compliance by external service providers on an ongoing basis: [Assignment: organization-defined processes, methods, and techniques].		
5.1	Are cloud-specific threats (e.g., misconfiguration of cloud resources, API vulnerabilities) explicitly addressed in threat models? RA-3 • **RA-3 (Risk Assessment)-** • The organization: • Conduct a risk assessment of the information system [Assignment: organization-defined frequency] • Document of the risk assessment results in a risk assessment report • Develops and implements a risk mitigation strategy; and		

Ref (AAIRAF)	Checklist Item	Assessor Rating (Y/N/P/NA)	Notes/Evidence
	• Reviews and updates the risk assessment [Assignment: organization-defined frequency] or whenever there are significant changes to the information system or environment of operation (e.g., new systems, applications, ports, protocols, services, or a change in the threat).		
5.1	Are cloud-native security controls (e.g., IAM, Network Security Groups, Cloud WAFs) leveraged for AI deployments? SC-7 • **SC-7 (System and Communications Protection) - Boundary Protection** • The organization: • Monitors and controls communications at the external managed interfaces to the system and at key internal managed interfaces within the system. • Implements subnetworks for publicly accessible system components that are [Selection (one): physically; logically] separated from internal organizational networks; and • Connects to external networks or systems only through managed interfaces consisting of boundary protection devices arranged in accordance with an organizational security architecture.		
5.1	Are data residency requirements for AI data in the cloud understood and met? SA-1		

Ref (AAIRAF)	Checklist Item	Assessor Rating (Y/N/P/NA)	Notes/Evidence
	• **SA-1 (System and Services Acquisition) - System Security and Privacy Policy and Procedures** • The organization: • Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles] a system security and privacy policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and • Implement procedures to operationalize the policy and associated controls.		
5.1	If using containers for AI services, are robust container security practices (e.g., vulnerability scanning of images, secure registries) in place? CM-6 • **CM-6 (Configuration Management) - Configuration Settings** • The organization: • Establishes and documents configuration settings for information technology products employed within the information system using [Selection: security configuration checklists; benchmarks; [Assignment: organization-defined configuration guidelines] that: • Reflect the intent of the security and privacy requirements outlined in applicable laws, Executive Orders, directives,		

Ref (AAIRAF)	Checklist Item	Assessor Rating (Y/N/P/NA)	Notes/Evidence
	regulations, policies, standards, and guidelines. • Are consistent with manufacturer- or developer-provided security guidance. • Consider the complete system, the intended system operational environment, and organization-defined non-security requirements; and • Are reviewed and updated [Assignment: organization-defined frequency]; and • Implements the configuration settings.		
5.1	Is network segmentation and isolation implemented for AI workloads within the cloud environment? SC-7 • **SC-7 (System and Communications Protection)- Boundary Protection** • The organization: • Monitors and controls communications at the external managed interfaces to the system and at key internal managed interfaces within the system • Implements subnetworks for publicly accessible system components that are [Selection (one): physically; logically] separated from internal organizational networks; and • Connects to external networks or systems only through managed interfaces consisting of boundary protection devices arranged in		

Ref (AAIRAF)	Checklist Item	Assessor Rating (Y/N/P/NA)	Notes/Evidence
	accordance with an organizational security architecture.		
5.1	Are cloud access keys/credentials securely managed and rotated? IA-5 • **IA-5 (Identification and Authentication)-Authenticator Management** • The organization manages information system authenticators (e.g., passwords, tokens, biometrics) by: • Implementing multifactor authentication for: • Network access to privileged accounts; and • Local access to privileged accounts. o Requiring users to change temporary passwords after initial password assignment o Prohibiting password reuse for a specified number of generations o Enforcing password minimum and maximum lifetime (i.e., password aging) o Implementing specified password strength and complexity requirements o Implementing cryptographically based mechanisms for authentication that meet applicable Federal Information Processing Standards (FIPS) or National Institute of Standards and		

Ref (AAIRAF)	Checklist Item	Assessor Rating (Y/N/P/NA)	Notes/Evidence
	Technology (NIST) approved cryptographic algorithms o Employing mechanisms for managing devices that perform authentication o Preventing the use of group authenticators o Hiding feedback of authentication information o Masking feedback of authentication information o Protecting wireless access using authentication and encryption that meets applicable Federal Information Processing Standards (FIPS) o Authorizing wireless access to the information system prior to allowing network access o Invalidating automatically, token-based authenticators upon successful authentication; and o Implementing [Assignment: organization-defined mechanisms] to protect authenticator feedback (e.g., masking authenticator feedback).		
5.1	Are cloud-specific logging and monitoring services (e.g., CloudTrail, Azure Monitor) configured for AI resources? SI-4 • **SI-4 (System and Information Integrity) - System Monitoring** • The organization:		

Ref (AAIRAF)	Checklist Item	Assessor Rating (Y/N/P/NA)	Notes/Evidence
	o Monitors the system to detect: • Attacks and indicators of potential attacks in accordance with the following monitoring objectives: [Assignment: organization-defined monitoring objectives]; and • Unauthorized local, network, and remote connections • b. Identifies unauthorized use of the system through the following techniques and methods: [Assignment: organization-defined techniques and methods] o c. Invokes internal monitoring capabilities or deploy monitoring devices: o Strategically within the system to collect organization-determined essential information; and o At ad hoc locations within the system to track specific types of transactions of interest to the organization o d. Analyzes detected events and anomalies o e. Adjusts the level of system monitoring activity when there is a change in risk to organizational operations and assets, individuals, other organizations, or the Nation o f. Obtains legal opinion regarding system monitoring activities; and		

Ref (AAIRAF)	Checklist Item	Assessor Rating (Y/N/P/NA)	Notes/Evidence
	○ g. Provides [Assignment: organization-defined system monitoring information] to [Assignment: organization-defined personnel or roles] [Selection (one or more): as needed; [Assignment: organization-defined frequency]].		

C.2. EMBEDDED SYSTEMS SPECIFIC CHECKS *(Only applicable if AI system is in an Embedded System Environment)*

Ref (AAIRAF)	Checklist Item	Assessor Rating (Y/N/P/NA)	Notes/Evidence
5.2	Are AI security controls designed to operate within the specific resource constraints (processing, memory, power) of the embedded system? PS-3 • **PS-3 (Personnel Security) - System Security and Privacy Engineering Principles** • The organization employs system security and privacy engineering principles in the specification, design, development, implementation, and modification of the system.		
5.2	Do AI security controls avoid interfering with the system's real-time performance requirements? PS-3 • **PS-3 (Personnel Security) - System Security and Privacy Engineering Principles**		

Ref (AAIRAF)	Checklist Item	Assessor Rating (Y/N/P/NA)	Notes/Evidence
	• The organization employs system security and privacy engineering principles in the specification, design, development, implementation, and modification of the system.		
5.2	Are physical security measures implemented to protect the embedded system from tampering or theft? SR-9 • **SR-9 (Supply Chain Risk Management) - Tamper Protection** • The organization implements a tamper protection program for the information system that: a. Prevents unauthorized physical access, modification, or disruption to the information system; b. Detects tamper events; and c. Includes notification of appropriate organizational officials of the tamper events and resulting actions taken.		

5.2	Are mechanisms in place for secure, limited-connectivity updates (e.g., over-the-air updates with cryptographic validation)? SI-2
	• **SI-2 (System and Information Integrity) - Flaw Remediation**
	• The organization:
	  ○ Identifies, reports, and corrects information system flaws in a timely manner
	  ○ Tests software and firmware updates related to flaw remediation for		

Ref (AAIRAF)	Checklist Item	Assessor Rating (Y/N/P/NA)	Notes/Evidence
	effectiveness and potential side effects before installation o Installs security-relevant software and firmware updates within [Assignment: organization-defined time period] of the release of the updates; and • d. Incorporates flaw remediation into the organizational configuration management process.		
5.2	Are unique threats to embedded systems (e.g., sensor spoofing, GPS jamming, direct model manipulation) explicitly addressed in threat models? RA-3(1) • **RA-3(Risk Assessment):** The organization assesses risk, to include: • (a) Identifying threat sources and events • (b) Determining the likelihood of threat events occurring • (c) Determining the adverse impacts resulting from the occurrence of threat events; and • Determining security risks (i.e., the magnitude of harm resulting from the occurrence of threat events and the likelihood of occurrence).		

Ref (AAIRAF)	Checklist Item	Assessor Rating (Y/N/P/NA)	Notes/Evidence
5.2	Are Hardware Security Modules (HSMs) or Trusted Platform Modules (TPMs) used to protect cryptographic keys and system integrity? IA-5(1) • **IA-5 (1) (Identification and Authentication) Authenticator Management:** The organization manages authenticators in accordance with the applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance. • **Cryptographic Key Establishment and Management:** The organization establishes and manages cryptographic keys used for authentication, in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance.		
5.2	Is secure boot implemented to prevent unauthorized code execution during startup? CM-7(1) • **CM-7 (1) (Configuration Management)*:*** The organization manages the configuration of the information system including hardware, software, firmware, and documentation in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidelines. • **Least Functionality:** The organization configures the information system to provide only essential capabilities and to prohibit or restrict the use of specified		

Ref (AAIRAF)	Checklist Item	Assessor Rating (Y/N/P/NA)	Notes/Evidence
	functions, ports, protocols, and services.		
5.2	Is all code (including AI models) cryptographically signed to ensure integrity? CM-5(4) • **CM-5 (4) Configuration Management:** The organization manages the configuration of the information system including hardware, software, firmware, and documentation in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidelines. • **Access Restrictions for Change Control:** The organization controls access to configuration management tools to prevent unauthorized modification of the information system.		

5.2	Are memory protection mechanisms implemented to prevent unauthorized access to sensitive data? SI-11(2) • **SI-11 (2) (System and Information Integrity) Information System Use:** • The organization: • **Memory Protection:** Implements memory protection mechanisms to protect system resources.		
5.2	Is anomaly detection implemented to identify unusual sensor data patterns or system behavior? SI-4(4) • **SI-4 (4)(System and Information Integrity):** The organization: • **Information System Monitoring:** Monitors the information system to detect: • (a) Attacks and indicators of potential attacks in accordance with [Assignment: organization-defined monitoring objectives]; and • (b) Information security flaws in accordance with [Assignment: organization-defined monitoring objectives].		
5.2	Are redundant and fail-safe mechanisms incorporated to ensure safe operation even under compromise? CP-2(6) • **CP-2 (6) (Contingency Planning):** The organization develops and implements a contingency plan for the information system that:		

	• **Redundancy and Failover:** Provides for redundant system elements and incorporates failover capabilities.		
5.2	Is strict access control implemented for the AI model and its parameters on the device? AC-3(1) • **AC-3 (1) (Access Control):** The organization: • **Access Enforcement:** Enforces approved authorizations for logical access to the information system and information within the system, in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance.		
5.2	Is there a reliable human override capability in case of AI malfunction or compromise? SA-11(1) • **SA-11 (1) (System and Services Acquisition) Developer Security Testing and Evaluation:** The organization tests and evaluates the information system, system component, or information system service for security flaws and establishes a process to rapidly address flaws that are discovered. • **Human in the Loop:** The organization employs human in the loop capabilities to assist with the performance of the function and ensure proper function and security of the information system.		
5.2	Are techniques like model obfuscation employed to make reverse-engineering of the AI model more difficult on the device? MP-7(1)		

	• **MP-7 (1) Media Protection:** The organization protects information system media containing organizational information. • **Output Handling:** The organization sanitizes, releases, and destroys information system media.		
5.2	Are communication protocols for the embedded system (e.g., between components, to command) secured against interception and manipulation? SC-8(1) • **SC-8 (1) (System and Communications Protection) Transmission Confidentiality and Integrity:** The organization protects the confidentiality and integrity of transmitted information. • **Cryptographic Protection:** The information system employs cryptographic mechanisms to prevent unauthorized disclosure and modification of transmitted information.		

SUPPLEMENTAL INTAKE QUESTIONS

Initiative/Release Background

Initiative/Release Background (Table 1)	
AI Model Name	
AI Model Version	
AI Model Vendor	
Type of System	☐ Standalone ☐ Isolated LAN ☐ LAN ☐ WAN ☐ Cloud ☐ Embedded System(Weapon, Healthcare, ICS, etc.)
AI Model Type	☐ OSS ☐ GOTS ☐ COTS ☐ Proof of Concept
Security Risks	*Provide any risks or impacts on the system, e.g., "Low risk due to install on isolated LAN not connected to internet. Please see attachment regarding security risks introduced by this new hardware/AI Model."*
CCB Approval Status & Date	*When were requirements vetted by official CCB stakeholders and what was the prioritization level*
Current Security Categorization of Impacted System(s)	*Example: MML*
AI Model Data Type Classification	*Are sensitive Data Types included (ie PII, PHI, etc)*
What are the mission requirements/justification driving the change?	*Provide as much detail as to what is driving this change, as well as applicable mission requirements. Example: AI Model X allows for accurate simulation of environmental conditions to properly test and evaluate countermeasure laser system performance.*
What is the mission impact(s) if not approved?	*Provide as much detail as possible as to the mission impacts if this change is not approved – "mission stoppage" is not suffice. Example: If not approved, vital verification and validation activities would not occur or data would not include atmospheric effects, the results of which could seriously affect countermeasure performance metrics.*
AI Model Features (What functions does it perform?)	
Description of Use (What will it be used for? If it will be modified, state what features will be modified and who will do it.)	
Other Software Dependencies (Is additional software that is not part of the installation package required to be installed)	☐ No ☐ Yes - List required software below: *If there are software dependencies, ensure the software is already on your approved SW list or you need to add it to the SIA.*
Software Licensing or SLA Requirements (CM-10)	Is this a licensed version of software or are there additional SLA Requirements to take into consideration?

	☐ No ☐ Yes - List SLA requirements. If license requirements state type:

AI Model Intake Questionnaire

AI Model Intake Questionnaire (Table 2)		
YES	**NO**	**Item Review & Actions**
		*Does the AI Model process/store/transmit PII/Other Sensitive Data Types **(SC-28)**
		*Vendor support offered **(SR-7)**
		Is the AIBOM Available for review to support the request? **(SA-4(9), CM-8, CM-2)** If Yes – please include with SIA*
		Does the AI model require administrator rights during operation? **(AC-6(8))**
		Does the model require individual accounts for operation/use? **(IA-5, IA-4(9)), AC-3, AC-6)**
		Does the AI Model require configuration steps or extra permissions for standard users to execute the software (e.g., manually creating directories or files, setting up another software to run, etc.)? **(CM-2, CM-3, CM-6)**
		*Does the AI Model product perform encryption using a cryptographic module as its primary function that has NOT been validated for compliance with FIPS 140-3? **(SC-13)** (http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.140-3.pdf)
		*Does the AI Model product use ports, protocols, and services (PPS) that are NOT acceptable, NOT a best practice PPSM (https://cyber.mil/ppsm/) **(SC-7, SC-8)**
		Is the software IA or IA enabled Product (See Guidance Below) Examples include Threat detection and anomaly detection; Malware analysis and classification, vulnerability management, security orchestration-automation and response (SOAR)
To verify whether an IA or IA enabled product is certified or evaluated, visit the common criteria website Common Criteria CC Portal (commoncriteriaportal.org) *According to CNSSP #11, 10 Jun 2013 (http://www.cnss.gov/CNSS/issuances/Policies.cfm) and DISA STIG Application Security & Development Checklist, ver 3, rel 10, 23 Jan 2015, IA Control DCAS-1, (http://iase.disa.mil/stigs/Documents/U_Application_Security_and_Development_V3R10_stig.ZIP) IA or IA enabled COTS products must be evaluated/validated by accredited commercial laboratories or the NIST and GOTS IA or IA enabled products must have be evaluated by NSA or in accordance with NSA-approved processes.*		

Foreign Ownership/Influence

Foreign Ownership/Influence (Table 3)		
YES	**NO**	**Item Review and Description**
		*Foreign Owned

If foreign developed, provide alternative US manufactured software, if available, and justification for not using US developed software. (SR-5)	*Remember, if foreign owned/developed, you must include any alternate US SW and why it is not being used. Note that use of any foreign software will lead to delays in processing as additional security approvals are required. Search this site for alternate solutions* https://alternativeto.net/

Vulnerability Check

Vulnerability Check (Table 4)	
***This list IS NOT all inclusive but is a starting point for the due diligence process. Included # and details for vulnerabilities found* (SA-5, RA-5)**	
WEBSITE	**RELEVANT VULNERABILITIES NOTED**
NIST National Vulnerability Database (NVD) http://web.nvd.nist.gov/view/vuln/search	
US-CERT Vulnerability Notes Database http://www.kb.cert.org/vuls/	
US-CERT Vulnerability Current Activity https://www.us-cert.gov/	
Common Vulnerabilities and Exposures http://cve.mitre.org/cve/	
Common Weakness Enumeration http://cwe.mitre.org/	
Common Attack Pattern Enumeration and Classification https://capec.mitre.org	
DoD Information Assurance Vulnerability Management (IAVM) Program https://iavm.csd.disa.mil/ (DoD Only)	
CVE Details http://www.cvedetails.com	
MITRE ATLAS https://atlas.mitre.org/	
Search Engine	