ASSESSMENT INTERVIEW QUESTION AND ANSWER SETS

This table is a set of question-and-answer pairs that equips assessors with supplemental assessment criteria for planning and conducting SCAs. Specifically, it contains canned interview questions, along with expected answers, detailing specifically how the control should be implemented for AI systems. Where [XYZ] appears, organizationally defined parameters shall be substituted, such as for agency-specific assignments. In some instances, an information type is shown inside square brackets – e.g., [methods], [processes], to further specify the type of information needed.

Control ID	Environment (infrastructure, network)	AI Platform (AI components, AI software)	AI Models (ML models, LLMs)	AI Data (training data, validation data)
AC-01-00	Q. What roles are used to restrict access to the AI environment and which users have them? A. The list of roles is [XYZ], and the users assigned to each role are [XYZ].	Q. What access control policies are specific to AI systems? A. AI-specific access control policies are [XYZ]. Q. What roles are used to restrict access to the AI Models and which users have them? A. The list of roles is [XYZ], and the users assigned to each role are [XYZ].	Q. What roles are used to restrict access to the AI Models and which users have them? A. The list of roles is [XYZ], and the users assigned to each role are [XYZ].	Q. What are the access control policies specific to AI training datasets in Production and lower environments? A. Access control policies specific to AI training datasets in Production and lower environments are [policies].
AC-02-12	Q. How are system accounts monitored for [atypical usage]? A. System accounts are monitored for [atypical usage]. Q. How is the atypical usage of system accounts reported to [personnel or roles]? A. Atypical usage of system accounts is reported to [personnel or roles].	Q. How are platform and application accounts monitored for [atypical usage]? A. System accounts are monitored for [atypical usage]. Q. How is the atypical usage of platform and application accounts reported to [personnel or roles]? A. Atypical usage of platform/application accounts is reported to [personnel or roles].		

'Approved for Public Release; Distribution Unlimited. Public Release Case Number 25-1028.

Control ID	Environment (infrastructure, network)	AI Platform (AI components, AI software)	AI Models (ML models, LLMs)	AI Data (training data, validation data)
AC-03-00	Q. How are authorizations for logical access to information and system resources authorized and enforced throughout the environment? A. Authorized access to the AI environment is enforced by [access control policies] using [access control methods]. Q. In the AI environment, how is access approved to the LLM chat to mitigate direct prompt injections? A. In the AI environment, access is approved via [method] for the LLM chat to mitigate direct prompt injections.	Q. How are authorizations for logical access to information and AI platform resources authorized and enforced? A. Authorized access to AI resources is enforced by [access control policies] using [access control methods]. Q. In the AI platform, how is access approved to the LLM chat to mitigate direct prompt injections? A. In the AI platform, access is approved via [method] for the LLM chat to mitigate direct prompt injections.	Q. How are authorizations for logical access to information within AI models authorized and enforced throughout the environment? A. Authorized access to the AI models is enforced by [access control policies] using [access control methods].	Q. How are authorizations for logical access to information and AI platform resources authorized and enforced? A. Authorized access to AI resources is enforced by [access control policies] using [access control methods]. Q. In the AI data, how is access approved to the LLM chat to mitigate direct prompt injections? A. In the AI data, access is approved via [method] for the LLM chat to mitigate direct prompt injections.
AC-04-00	Q. How is information flow controlled to prevent sensitive information from being disclosed to those that do not require access to it? A. Information flow is controlled by [means].	Q. How does the AI platform controls information flow to prevent sensitive information from being disclosed? A. The AI Platform controls information flow by [means].	Q. How does the AI Model controls information flow to prevent sensitive information from being disclosed? A. The AI Model controls information flow by [means].	Q. How is AI Data protected to prevent sensitive information from being disclosed? A. AI Data is protected by [methods] to prevent sensitive information from being disclosed.
AC-04-09		Q. How are human reviews of the AI platform performed with regards to information flow enforcement? A. Human review is enforced for [selected processes] under [conditions].		
AC-04-15		Q. How is the transfer of unsanctioned information between security domains detected and prevented? A. Unsanctioned information is detected by [methods] and its transfer between security domains is prevented in accordance with [security and/or privacy policy].		
AC-04-25	Q. How is information within the environment sanitized to minimize harmful or malicious code? A. Data within the AI environment is sanitized to minimize transfer of [malware/command and control code/ encoded data, sensitive data] according to [policy].	Q. How is data flowing within the AI platform sanitized by malicious code or destroyed when no longer in service? A. Data on AI platforms is [sanitized/destroyed] to minimize transfer of [malware/command and control code/ encoded data, sensitive data] according to [policy].	Q. How is AI model data sanitized to prevent the flow of sensitive data and/or destroyed when no longer in service? A. AI model data is sanitized of sensitive data according to [policy] or destroyed according to [guidelines].	Q. How is AI data sanitized to prevent the flow of sensitive data and/or destroyed when no longer in service? A. AI training data is sanitized of sensitive data according to [policy] or destroyed according to [guidelines].

Control ID	Environment (infrastructure, network)	AI Platform (AI components, AI software)	AI Models (ML models, LLMs)	AI Data (training data, validation data)
AC-05-00	Q. What kind of roles/groups are used to limit access to AI environment and which users are members of each of those groups? A. The groups to limit access are [XYZ] and the users in each group are [XYZ].	Q. What kind of roles/groups are used to limit access to AI platform and which users are members of each of those groups? A. The groups to limit access are [XYZ] and the users in each group are [XYZ]. Q. How is the principle of separation of duties applied to the LLM? A. Separation of duties is achieved by means of [XYZ}.	Q. What kind of roles/groups are used to limit access to AI Models and which users are members of each of those groups? A. The groups to limit access are [XYZ] and the users in each group are [XYZ].	

Control ID	Environment (infrastructure, network)	AI Platform (AI components, AI software)	AI Models (ML models, LLMs)	AI Data (training data, validation data)
AC-06-00	Q. What permissions are assigned to each of the groups/roles that are used to limit access to the AI environment? Do any roles exceed necessary access permissions? A. Access to AI environment is enforced by [using/not using] least privilege access. Users [do/do not] only have access to systems necessary to perform their duties. Permissions for each of the groups are [XYZ]. Q. What permissions are assigned to each user/group/role to prevent the disclosure of sensitive information? A. Permissions assigned to each user/group/role are [XYZ]. Q. What permissions are granted to plugins, and how are they managed to prevent excessive privilege? A. Permissions for each plugin are [XYZ]. When new plugins are needed the process to assign privilege is [XYZ].	Q. What permissions are assigned to each of the groups/roles that are used to limit access to the AI platform? Do any roles exceed the necessary access permissions? A. Access to AI platform is enforced by [using/not using] the principle of least privilege. Users [do/do not] only have access to systems necessary to perform their duties. Permissions for each of the groups are [XYZ]. Q. Within the AI platform, what limitations are implemented to prevent the chat plugin from accessing sensitive information? A. [XYZ] limitations are implemented to prevent the chat plugin from accessing sensitive information within the AI platform. Q. What permissions are assigned to the AI Platform to prevent the disclosure of sensitive information? A. Permissions assigned to the AI Platform are [XYZ]. Q. What kind of controls are in place to prevent LLMs from having excessive autonomy and to limit access to only needed information? A. The following [XYZ] processes and procedures are in place to prevent the LLM from having too much autonomy. Additionally, the following [XYZ] permissions are in place to limit which data they may access. Q. What permissions, and how are they managed and assigned to LLM plugins to prevent excessive permissions? A. Permissions for each of the plugins are [XYZ]. When new plugins are needed the process to assign privileges is [XYZ].	Q. What permissions are assigned to each of the groups/roles that are used to limit access to the AI Models? Do any roles exceed necessary access permissions? A. Access to AI models is enforced by [using/not using] least privilege access. Users [do/do not] only have access to systems necessary to perform their duties. Permissions for each of the groups are [XYZ]. Q. What permissions are assigned to the AI Model to prevent the disclosure of sensitive information? A. Permissions assigned to the AI Model are [XYZ].	Q. What permissions are assigned to each of the groups/roles that are used to limit access to the AI and LLM training data? Do any roles exceed the necessary access permissions? A. Access to AI training data is enforced by [using/not using] least privilege access. Users [do/do not] only have access to systems necessary to perform their duties. Permissions for each of the groups are [XYZ]. Q. What permissions are assigned to AI Data to prevent the disclosure of sensitive information? A. Permissions assigned to the AI Data are [XYZ].

Control ID	Environment (infrastructure, network)	AI Platform (AI components, AI software)	AI Models (ML models, LLMs)	AI Data (training data, validation data)
AC-07-00	Q. How many concurrent sessions can a user of the AI have at the same time? A. Users can have [XYZ] number of concurrent sessions, while using the AI. Q. Are users of the AI automatically disconnected if they are inactive for more than [XYZ] number of minutes? A. Users are disconnected after [XYZ] number of minutes. Q. What steps are being taken to prevent malicious users from using techniques such as (CAPTHCA, Deep Fakes, Identity Spoofing, Synthetic Identities) from logging into the AI environment? A. [steps] are being taken to prevent malicious users from using techniques such as (CAPTHCA, Deep Fakes, Identity spoofing, Synthetic identities) from logging into the AI environment.	Q. What steps are being taken to prevent malicious users from using techniques such as (CAPTHCA, Deep Fakes, Identity Spoofing, Synthetic Identities) from logging into the AI platform? A. [steps] are being taken to prevent malicious users from using techniques such as (CAPTHCA, Deep Fakes, Identity spoofing, Synthetic identities) from logging into the AI platform.		
AC-12-00		Q. How are user sessions terminated such that processing by AI components does not continue past the end of the user session? A. AI sessions are terminated according to [conditions/triggers/policy].		
AC-14-00	Q. Which parts, if any, of the environment are accessible without user authentication? A. The areas that do not require authentication are [list]. Q. What permitted actions are allowed within a system without identification or authentication within the AI environment? A. The [actions] are permitted without identification or authentication within the AI environment.	Q. Which parts of the AI are accessible without user authentication? A. The functions that do not require authentication are [list]. Q. What permitted actions are allowed within a system without identification or authentication within the AI platform? A. The [actions] are permitted without identification or authentication within the AI platform.		Q. What kind of user authentication is required to access the AI training data, and who can access this data? A. Users are required to use the following authentication methods [XYZ], and the users that have access to the AI training data are [XYZ].

Control ID	Environment (infrastructure, network)	AI Platform (AI components, AI software)	AI Models (ML models, LLMs)	AI Data (training data, validation data)
AC-17-00	Q. How is remote access from external networks to the environment restricted? What access controls are in effect to only allow authorized parties from accessing the environment? Which mechanisms are employed to facilitate secure and encrypted remote access while allowing for visibility to scan and detect malicious code/files. A. Environment remote access is restricted by [XYZ]. The access controls in effect at the environment are [controls (CA-3)]. The mechanisms in use to facilitate secure remote connections are [mechanisms].	Q. How is remote access to AI components (platform) restricted from external networks? What access controls are in effect to only allow authorized parties from accessing the AI platform? Which mechanisms are employed to facilitate secure and encrypted remote access while allowing for visibility to scan and detect malicious code/files. A. AI component remote access is restricted by [XYZ]. The access controls in effect at the AI platform are [controls (CA-3)]. The mechanisms in use to facilitate secure remote connections are [mechanisms].		
AC-20-00	Q. How is access to the AI environment and its components restricted from external access? A. The following [restrictions] are in place to ensure that access from external systems is not possible. Q. When connected to the environment, are there any external services (i.e. Internet, networks not part of the system) that can be accessed? If yes, which services can be accessed and why? A. Yes/No. If yes, you can access [XYZ] for the following [purposes].	Q. How is access to the AI platform restricted from external access? A. The following [restrictions] are in place to ensure that access from external systems is not possible.	Q. How is access to the AI models restricted from external access? A. The following [restrictions] are in place to ensure that access from external systems is not possible.	Q. How is access to AI, production, model, and validation data restricted from external access? A. The following [restrictions] are in place to ensure that access from external systems is not possible.
AC-21-00	Q. How is information sharing with other organizations (internal or external) restricted and reviewed to minimize the possibility of sensitive information being invertedly disclosed? A. We review information that is being shared by [means]. Sensitive information is restricted in the following [manner].	Q. What kind of protections does the AI platform provide to protect against sensitive information disclosure? A. The AI platform provides the following [safeguards] to protect against inadvertent sensitive information disclosure.		Q. How is data sanitized to prevent the disclosure of sensitive information? A. Data is sanitized by [methods].

Control ID	Environment (infrastructure, network)	AI Platform (AI components, AI software)	AI Models (ML models, LLMs)	AI Data (training data, validation data)
AC-23-00		Q. How is the platform protected from data mining by agents attempting to find patterns in the AI platform? A. The platform is protected from adversarial data mining by [methods].		
AC-24-00	Q. Is access control enforced prior to each access request and limited to only authorized actions and users? A. Access control is enforced prior to access requests by [methods and/or mechanisms] for authorized actions and users.	Q. Is access control enforced prior to each access request and limited to only authorized actions and users? A. Access control is enforced prior to access requests by [methods and/or mechanisms] for authorized actions and users.		
AT-03-00			Q. What kind of security training is provided to personnel involved in AI development, deployment, and maintenance, in terms of how AI Models should be protected? A. We provide the following [training] to all personnel involved in the life cycle of the AI.	Q. What kind of security training is provided to personnel involved in AI development, deployment, and maintenance, in terms of how production AI training data should be protected? A. We provide the following [training] to all personnel involved in the life cycle of the AI.

Control ID	Environment (infrastructure, network)	AI Platform (AI components, AI software)	AI Models (ML models, LLMs)	AI Data (training data, validation data)
AU-02-00	Q. What kinds of events on the environment is the system capable of logging to support auditing? What channels are used to coordinate logging functions with other organizational entities to provide audit-related info to inform selection of logging criteria? Are the selected event criteria for logging sufficient for supporting after-the-fact investigations, and how would the audit trail be used to reconstruct an incident. A. At the environment level we log [list of events]. The events are communicated to other organizational entities to inform them of their selection of logging criteria. The data selected for logging is sufficient for conducting investigations because [reasons], as the [specific logs] can construct a cohesive audit trail.	Q. What kinds of events on the platform is the system capable of logging to support auditing? What channels are used to coordinate logging functions with other organization entities to provide audit related info to inform selection of logging criteria? Are the selected event criteria for logging sufficient for supporting after-the-fact investigations, and how would the audit trail be used to reconstruct an incident. A. The platform is capable of logging [capabilities], and it is used to log [selected event criteria]. These events are communicated to other organizational entities to inform their selection of logging criteria. The data selected for logging is sufficient for conducting investigations because [reasons], as the [specific logs] can construct a cohesive audit trail.	Q. What types of events related to access and use of AI models are logged? A. The [types of events] are logged.	Q. What types of events related to access and use of AI data are logged? A. The [types of events] are logged.
AU-03-00			Q. What kind of information is logged with regards to access to AI Models? A. The [list of information types] are logged with, at a minimum, time stamps, who accessed, and what kind of action was taken.	Q. What kind of information is logged with regards to access to AI Data? A. The [list of information types] are logged with, at a minimum, time stamps, who accessed, and what kind of action was taken.
AU-06-00		Q. What kind of audit records are generated for the chat plugin in the AI platform? A. The [kinds of audit records] are generated for the chat plugin in the AI platform. Q. What kind of audit records are generated by the AI platform when sensitive information is accessed? A. The [kinds of audit records] audit records are generated by the AI platform when sensitive information is accessed.		

Control ID	Environment (infrastructure, network)	AI Platform (AI components, AI software)	AI Models (ML models, LLMs)	AI Data (training data, validation data)
AU-06-05	Q. How are audit records analyzed to identify inappropriate or unusual activity in the environment? A. Audit records are analyzed to identify inappropriate or unusual activity in the environment by [methods].	Q. How are audit records analyzed to identify inappropriate or unusual activity in the platform? A. Audit records are analyzed to identify inappropriate or unusual activity in the platform by [methods].		
AU-09-00		Q. What are the means of protecting audit information and logging tools from unauthorized access, modification, and deletion on the AI platform? A. Audit information and logging tools are protected through [means]. Alerts are generated upon discovery of unauthorized access, modification, and deletion of audit information.		Q. What are the means of protecting audit information from unauthorized access, modification, and deletion in the AI data. A. Audit information of AI data is protected through [means]. Alerts are generated upon discovery of unauthorized access, modification, and deletion of audit information.
CA-02-00	Q. What kinds of assessment procedures are used to ensure that security concerns are properly tested for the AI environment? A. The [list of procedures] are followed.	Q. What kinds of assessment procedures are used to ensure that security concerns are properly tested for the AI platform? A. The [list of procedures] are followed. Q. What assessment procedure checks are there to ensure bias has not been introduced into the AI platform? A. The [assessment procedure checks] are implemented to ensure bias has not been introduced into the AI platform.	Q. What kinds of assessment procedures are used to ensure that security concerns are properly tested for the AI models? A. The [list of procedures] are followed. Q. What assessment procedure checks are there to ensure bias has not been introduced into the AI models? A. The [assessment procedure checks] are implemented to ensure bias has not been introduced into the AI models.	Q. What kinds of assessment procedures are used to ensure that security concerns are properly tested for the AI data? A. The [list of procedures] are followed. Q. What assessment procedure checks are there to ensure bias has not been introduced into the AI data? A. The [assessment procedure checks] are implemented to ensure bias has not been introduced into the AI data.
CA-08-00	Q. How often are penetration tests performed on the AI environment? What is the scope of the penetration testing? A. Penetration testing is performed at [frequency]. The scope of these tests include [scope].	Q. How often are penetration tests performed on the AI platform? What is the scope of the penetration testing? A. Penetration testing is performed at [frequency]. The scope of the tests include [scope].		

'Approved for Public Release; Distribution Unlimited. Public Release Case Number 25-1028.

Control ID	Environment (infrastructure, network)	AI Platform (AI components, AI software)	AI Models (ML models, LLMs)	AI Data (training data, validation data)
CA-09-00	Q. Provide documentation of all internal system interfaces, including all AI components, that show the interface characteristics, security and privacy requirements, and the nature of the information communicated. A. The SSP and [other documents] show all internal interfaces, ports, and protocols. Q. How often is interface documentation reviewed? A. We review interface documentation [frequency].			
CM-02-00		Q. What baseline configuration is used to determine if bias was introduced into the AI platform? A. [baseline configurations] were used to determine if bias was introduced into the AI platform.	Q. What baseline configuration is used to determine if bias was introduced into the AI models? A. [baseline configurations] were used to determine if bias was introduced into the AI models.	Q. What baseline configuration is used to determine if bias was introduced into the AI data? A. [baseline configurations] were used to determine if bias was introduced into the AI data.
CM-03-00	Q. What kind of documentation is needed to request changes to the environment? A. The [set of documents] is needed for all proposed changes, including type of change, justification, testing procedures, and possible effects on other components.	Q. What documentation is needed to request changes to the AI platform? A. The [set of documents] is needed for all proposed changes, including type of change, justification, testing procedures, and possible effects on other components.		
CM-05-00	Q. What is the change management process associated with the AI environment, concerning changes to the hardware or firmware defined, documented, and enforced? A. The process to make changes to the environment is [XYZ]. This process [is/is not] documented, and [does/does not] require approval and enforcement of physical and logical access restrictions associated.	Q. How is the change management process associated with the AI platform or software defined, documented, and enforced? A. The process to make changes to the platform or software is [XYZ]. This process [is/is not] documented, and [does/does not] require approval and enforcement of physical and logical access restrictions associated. Q. How are changes to the chat plugin authorized within the AI platform? A. Changes to the chat plugin are authorized via [methods] within the AI platform.	Q. What is the change management process associated with systems that house AI Models? A. The process to make changes to the models(s) is [XYZ]. This process [is/is not] documented, and [does/does not] require approval and enforcement of physical and logical access restrictions associated.	

Control ID	Environment (infrastructure, network)	AI Platform (AI components, AI software)	AI Models (ML models, LLMs)	AI Data (training data, validation data)
CM-07-00	Q. How can you access the environment that hosts the AI network? Include network protocols, locations, what permissions are needed, what controls mechanisms are in place. A. Access to the AI environment can be obtained via the [protocols], from the [network segments] and the [permissions] associated with your account. Enforcement is done via [methods]. Q. How is access to LLM plugins restricted? A. The following [XYZ] restrictions are in place to limit access to the LLM plugins.	Q. How can you access the system(s) that host the AI platform? Include network protocols, locations, what permissions are needed/ not needed to limit model access to necessary features, what controls mechanisms are in place. A. Access to the systems that host AI Platform can be obtained via the [protocols], from the [network segments] and the [permissions] associated with your account. Enforcement is done via [methods]. Q. How does the AI Platform restrict the information that LLM plugins can access? A. The platform restricts access to the LLM plugins by [methods].	Q. How can you access the system(s) that host AI Models? Include network protocols, locations, what permissions are needed/ not needed to limit model access to necessary features, what controls mechanisms are in place. A. Access to the systems that host AI Models can be obtained via the [protocols], from the [network segments] and the [permissions] associated with your account. Enforcement is done via [methods].	Q. How is access to training data restricted? A. Access to training data is restricted by [means].
CM-11-00	Q. Describe how users are prevented from installing software on the systems or introducing new tools/executables onto the environment? A. The [mitigations] are in place to ensure that users cannot install or introduce new tools to the environment. Q. What is the process that is followed before new software can be installed or new tools/executables can be introduced? A. The [process] ensures that users cannot install or introduce new tools to the environment. Q. How often are software and tools installed or copied to the environment reviewed to ensure that they are still needed? A. We review tools/executables used on the system on a [frequency] basis to make sure that they are still needed and safe.	Q. Describe how users are prevented from installing software on the systems or introducing new tools/executables onto the AI platform? A. The [mitigations] are in place to ensure that users cannot install or introduce new tools to the AI Platform. Q. What is the process that is followed before new software can be installed or new tools/executables can be introduced? A. The [process] ensures that users cannot install or introduce new tools to the AI Platform. Q. How often are software and tools installed or copied to the environment reviewed to ensure that they are still needed? A. We review tools/executables used on the system on a [frequency] basis to make sure that they are still needed and safe.		

Control ID	Environment (infrastructure, network)	AI Platform (AI components, AI software)	AI Models (ML models, LLMs)	AI Data (training data, validation data)
CM-13-00		Q. How are system data actions that process PII and FTI mapped and documented for the AI platform? A. System data actions that process PII and FTI are mapped and documented for the AI platform by [methods].		
CM-14-00	Q. What is the process to install patches to the infrastructure components? A. The [process] is used to install patches.	Q. What is the process to install patches to the AI platform and its components? A. The [process] is used to install patches.		
CP-01-00	Q. What are the contingency plans to follow in case of an emergency and how are they disseminated to the appropriate personnel? A. Contingency plans are included in [set of documents] and they are provided to all necessary users via [methods].	Q. What are the contingency plans to follow in case of an emergency and how are they disseminated to the appropriate personnel? A. Contingency plans are included in [set of documents] and are provided to all necessary users via [methods].		
CP-09-00	Q. How are backups of AI Environment made? A. The AI environment is backed up using [methods and schedule].	Q. How are backups of the AI platform made? A. The platform is backed up using [methods and schedule].	Q. How are backups of the AI models made? A. The AI models are backed up using [methods and schedule].	Q. How are backups of AI Data made? A. The AI data is backed up using [methods and schedule].
IA-02-00	Q. How are users with access to the environment managed, authenticated, reviewed, and vetted to ensure that they require access? A. The [process] is used to add new users, and they are authenticated via [confirmation methods], and we review user accesses on a [frequency] to ensure that they still require access, if they do not require access we remove them. Q. In the AI environment, in what way is AI being used to authenticate as well as confirm the user is a human? A. Accounts are uniquely identified and authenticated as real people via [methods].	Q. How are users with access to the AI Platform managed, authenticated, reviewed, and vetted to ensure that they require access? A. The [process] is used to add new users, and they are authenticated via [methods], and we review user access on a [frequency] to ensure that they still require access, if they do not require access we remove them. Q. In the AI platform, in what way is AI being used to authenticate as well as confirm the user is a human? A. Accounts are uniquely identified and authenticated as real people via [methods].		

Control ID	Environment (infrastructure, network)	AI Platform (AI components, AI software)	AI Models (ML models, LLMs)	AI Data (training data, validation data)
IA-02-01	Q. How is multi-factor authentication implemented for privileged accounts within the AI environment? A. Multi-factor authentication is implemented via [methods] for privileged accounts within the AI environment. Q. Is the system following NIST 800-63-3 in its choices for multi-factor authentication within the AI environment? A. The system follows [NIST-800-63-3] in its choices for multi-factor authentication within the AI environment.	Q. Is the system following NIST 800-63-3 in its choices for multi-factor authentication within the AI platform? A. The system follows [NIST-800-63-3] in its choices for multi-factor authentication within the AI platform.		
IA-02-02	Q. Is the system following NIST 800-63-3 in its choices for multi-factor authentication within the AI environment? A. The system follows [NIST-800-63-3] in its choices for multi-factor authentication within the AI environment.	Q. Is the system following NIST 800-63-3 in its choices for multi-factor authentication within the AI platform? A. The system follows [NIST-800-63-3] in its choices for multi-factor authentication within the AI platform.		
IA-03-00	Q. How are devices uniquely identified and authenticated before establishing a connection to an environment containing AI systems? A. Devices are uniquely identified by [methods/ identifiers] and authenticated by [methods].			
IA-06-00	Q. How is the feedback of authentication information, during the authentication process, protected from possible disclosure to and exploitation from unauthorized parties? A. Feedback from authentication information is protected by [methods].			

Control ID	Environment (infrastructure, network)	AI Platform (AI components, AI software)	AI Models (ML models, LLMs)	AI Data (training data, validation data)
IA-08-00	Q. Do you have any external users that use the environment? If so, how do you identify them? A. We [do/do not] have external users. (If yes) Users are identified via [methods] and they are required to register by [methods]. Q. How are non-organizational users uniquely identified and authenticated within the AI environment? A. Non-organizational users are uniquely identified and authenticated via [methods].	Q. Do you have any external users that use the AI Platform? If you do, how do you identify them? A. We [do/do not] have external users. (If yes) Users are identified via [methods] and they are required to register by [methods]. Q. How are non-organizational users uniquely identified and authenticated within the AI platform? A. Non-organizational users are uniquely identified and authenticated via [methods].		
IA-12-00	Q. How do you validate the identity of a user who is attempting to access the AI environment with the following threats? [Deep fakes, Identity spoofing, Synthetic identity, CAPTCHA]? A. We validate the identity of the user using the following trusted sources of identity matching. We also ensure that the person is physically present at the point of verification when employing biometrics.	Q. How do you validate the identity of a user who is attempting to access the AI platform with the following threats? [Deep fakes, Identity spoofing, Synthetic identity, CAPTCHA]? A. We validate the identity of the user using the following trusted sources of identity matching. We also ensure that the person is physically present at the point of verification when employing biometrics.		
MA-03-00	Q. What is the process to install system patches to the production environment? A. The [process] is used to install patches.	Q. What is the process to install patches to the production AI platform? A. The [process] is used to install patches.		

Control ID	Environment (infrastructure, network)	AI Platform (AI components, AI software)	AI Models (ML models, LLMs)	AI Data (training data, validation data)
MA-05-00	Q. What is the process to authorize maintenance personnel that will be accessing the environment? A. The [process] is used for authorizing maintenance personnel. Q. What is the process to ensure that maintenance personnel only have access to the components needing maintenance? A. Maintenance personnel are escorted while performing their duties by someone from the internal team to ensure that they do not attempt to access other parts of the environment.	Q. What is the process to authorize maintenance personnel that will be accessing the AI platform? A. The [process] is used for authorizing maintenance personnel. Q. What is the process to ensure that maintenance personnel only have access to the components needing maintenance? A. Maintenance personnel are escorted while performing their duties by someone from the internal team to ensure that they do not attempt to access other parts of the platform.		
MA-06-00	Q. How often are patches applied to devices (physical or virtual) in the environment? A. Patches are applied on a [frequency] basis.	Q. How often are patches applied to the AI platform? A. Patches are applied on a [frequency] basis.		
PE-11-00	Q. What backup power procedures are in place? A. The [procedures] are in place deal with power loss situations. [Consider AI architectures designed to adequately allow for checkpoint and restore operations in case of loss or corruption due to power loss]			
PL-02-00		Q. How is the context of AI usage and inventory biases reviewed? A. Context of AI usage to ascertain and inventory biases is reviewed using [documents]. Q. What security and privacy plans have been implemented to ensure bias is not introduced into the AI platform? A. The [security and privacy plan] has been implemented to ensure bias has not been introduced into the AI platform.	Q. What security and privacy plans have been implemented to ensure bias is not introduced into the AI models? A. The [security and privacy plan] has been implemented to ensure bias has not been introduced into the AI models.	Q. What security and privacy plans have been implemented to ensure bias is not introduced into the AI data? A. The [security and privacy plan] has been implemented to ensure bias has not been introduced into the AI data.

Control ID	Environment (infrastructure, network)	AI Platform (AI components, AI software)	AI Models (ML models, LLMs)	AI Data (training data, validation data)
PL-04-00		Q. What methods are used to prevent bias from entering AI platforms and software? A. Bias is prevented from entering AI platform and software by [methods].	Q. What methods are used to prevent bias from entering AI models? A. Bias is prevented from entering AI models by [methods].	Q. What methods are used to prevent bias from entering the AI datasets? A. Bias is prevented from entering AI datasets by [methods].
PL-08-00	Q. What safeguards are in place to protect personally identifiable information? A. The [safeguards] are in place to protect PII.			
PM-07-00	Q. How is information privacy being protected? A. Information privacy is being protected by [methods].			
PM-12-00	Q. Describe the insider threat program that is in place and how it is used to safeguard the AI Environment. A. The [insider threat program] is in place and safeguards the AI environment using [methods]. (There is a good chance that you would be referred to a separate group/document that handles/describes this)	Q. Describe the insider threat program that is in place and how it is used to safeguard the AI platform. A. The [insider threat program] is in place and safeguards the AI Platform using [methods]. (There is a good chance that you would be referred to a separate group/document that handles/describes this)	Q. Describe the insider threat program that is in place and how it is used to safeguard the AI models. A. The [insider threat program] is in place and safeguards the AI models using [methods]. (There is a good chance that you would be referred to a separate group/document that handles/describes this)	Q. Describe the insider threat program that is in place and how it is used to safeguard the AI data. A. The [insider threat program] is in place and safeguards the AI datasets using [methods]. (There is a good chance that you would be referred to a separate group/document that handles/describes this)
PM-18-00	Q. What is the information privacy plan? A. The privacy plan is [XYZ].			
PM-30-00			Q. How is supply chain risk associated with the development, acquisition, maintenance, and disposal of AI Models managed? A. The supply change risk management strategy is [XYZ]. (It should include definitions for what acceptable risks are)	
RA-03-00	Q. What is the risk assessment process for the AI environment? A. The risk assessment process is [XYZ]. (ensure that threats and vulnerabilities are identified, also there should be an assessment of the likelihood of exploitation, possible effects in case of a successful attack)	Q. What is the risk assessment process for the AI platform? A. The risk assessment process is [XYZ]. (ensure that threats and vulnerabilities are identified, also there should be an assessment of the likelihood of exploitation, possible effects in case of a successful attack)		

Control ID	Environment (infrastructure, network)	AI Platform (AI components, AI software)	AI Models (ML models, LLMs)	AI Data (training data, validation data)
RA-05-00	Q. By what frequency, or randomized protocol, are vulnerabilities monitored and scanned for within the system and hosted applications? A. The system and hosted applications are scanned at [frequency] or [randomized using XYZ]. Q. What tools and processes are employed to scan for vulnerabilities within the environment? How is interoperability among tools ensured, and parts of the vulnerability management process automated to update vulnerabilities to be scanned as well as [standards 1-3]? A. The [tools] are used within the environment to scan for vulnerabilities, and the [processes] are used. Interoperability is facilitated between tools by [configurations/process]. The parts of the management process that are automated are [automated processes]. The list of vulnerabilities to be scanned [is/is not] automatically updated. Q. What is the process that is undertaken when a vulnerability is detected? How is information shared across systems to help eliminate similar vulnerabilities? A. When a vulnerability is detected in the environment, it [is/is not] remediated using [XYZ] based on defined risk. Information [is/is not] shared throughout the organization using [XYZ].	Q. By what frequency, or randomized protocol, are vulnerabilities monitored and scanned for on the AI platform? A. The AI platform is scanned at [frequency] or [randomized using XYZ]. Q. What tools and processes are employed to scan for vulnerabilities on the AI platform? How is interoperability among tools ensured, and parts of the vulnerability management process automated to update vulnerabilities to be scanned as well as [standards 1-3]? A. The [tools] are used to scan for vulnerabilities on the AI platform, and the [processes] are used. Interoperability is facilitated between tools by [configurations/process]. The parts of the management process that are automated are [automated processes]. The list of vulnerabilities to be scanned [is/is not] automatically updated. Q. What is the process that is undertaken when a vulnerability is detected? How is information shared between teams managing various AI tools to help eliminate similar vulnerabilities? A. When a vulnerability is detected in the environment, it [is/is not] remediated using [XYZ] based on defined risk. Information [is/is not] shared throughout the organization using [XYZ].		

Control ID	Environment (infrastructure, network)	AI Platform (AI components, AI software)	AI Models (ML models, LLMs)	AI Data (training data, validation data)
SA-03-02		Q. What is the approval process and documentation requirement for the use of live data in the preproduction AI platform? A. Approval is granted for the use of live data in preproduction AI platform according to [guidelines] and live data is protected with [controls].	Q. What is the approval process and documentation requirement for the use of live data in preproduction AI models? A. Approval is granted for the use of live data in preproduction AI models according to [guidelines] and live data is protected with [controls].	Q. What is the approval process and documentation requirement for the use of live data in preproduction AI datasets? A. Approval is granted for the use of live data in preproduction AI datasets according to [guidelines] and live data is protected with [controls].
SA-08-00		Q. How should AI systems be designed resiliently, with the ability to detect, respond to, and recover from disruptions and failures in a timely and effective manner? A. AI systems are designed resiliently, with the ability to detect using [methods], respond to using [methods], and recover from disruptions and failures in a timely and effective manner using [methods]. Q. What systems security and privacy engineering principles are applied when designing plugins? A. The [systems security and privacy engineering principles] are applied during design.	Q. How should AI systems be designed resiliently, with the ability to detect, respond to, and recover from disruptions and failures in a timely and effective manner? A. AI systems are designed resiliently, with the ability to detect using [methods], respond to using [methods], and recover from disruptions and failures in a timely and effective manner using [methods].	Q. How should AI systems be designed resiliently, with the ability to detect, respond to, and recover from disruptions and failures in a timely and effective manner? A. AI systems are designed resiliently, with the ability to detect using [methods], respond to using [methods], and recover from disruptions and failures in a timely and effective manner using [methods].
SA-09-00		Q. Do external providers of AI-enabled Privacy Enhancing Technologies (PETs) systems and services comply with agency [security and privacy requirements]. A. External providers of PETs must comply with [policies]. Q. How is access and documentation of trustworthiness for external model sources recorded? A. Access and documentation of trustworthiness for external model sources are recorded via [methods].		

Control ID	Environment (infrastructure, network)	AI Platform (AI components, AI software)	AI Models (ML models, LLMs)	AI Data (training data, validation data)
SA-09-05		Q. How is the location of information processing, data storage, and system services being managed and controlled through an external provider? A. The location of information processing, data storage, and system services is managed by the external provider according to organizationally defined [criteria].		
SA-09-06				Q. How is control of cryptographic keys for encrypted AI data transmitted through external systems maintained? A. Exclusive control of cryptographic keys is maintained by [internal methods].
SA-09-08				Q. Where is AI data physically stored? A. Physical storage of AI data is contained exclusively within the legal jurisdictional boundary of the United States in [locations].
SA-10-00		Q. How are changes to the AI platform tracked? A. The [processes] are used to track changes to the AI platform. Q. How are security flaws tracked by the developer/vendor? A. The [processes] are used to track flaws. (ensure that this includes how flaws are fixed). Q. How is retrained data and development to model configurations updated within the AI platform to prevent AI bias? A. Retrained data and development to model configurations is updated via [methods] within the AI platform to prevent AI bias.	Q. How does the system audit model predictions for fairness and equity? A. The system regularly audits model predictions for fairness and equity via [methods]. Q. How is retrained data and development to model configurations updated within the AI models to prevent AI bias? A. Retrained data and development to model configurations is updated via [methods] within the AI models to prevent AI bias.	Q. How is retrained data and development to model configurations updated within the AI data to prevent AI bias? A. Retrained data and development to model configurations is updated via [methods] within the AI data to prevent AI bias.

Control ID	Environment (infrastructure, network)	AI Platform (AI components, AI software)	AI Models (ML models, LLMs)	AI Data (training data, validation data)
SA-17-00	Q. How is access limited to the architecture of the system? A. Access to the architecture of the system is limited via [methods].	Q. Has the inclusion of AI-enabled PETs systems been vetted against the agency Enterprise Architecture? A. The agency Enterprise Architecture has vetted the use of PETs in the system. Q. How is access limited to model weights and hyperparameters of the system? A. Access to the model weights and hyperparameters are limited via [methods].		
SA-22-00	Q. What is the process to replace components that are no longer supported by the vendor? A. When an environment component is no longer supported the process of finding a replacement is [methods]. (this plan should include mitigations to be used while considering new components)	Q. What is the process to replace AI platform components that are no longer supported by the vendor? A. When an environment component is no longer supported the process of finding a replacement is [methods]. (this plan should include mitigations to be used while considering new components)		
SC-02-00	Q. How is system management functionality of the AI environment separated from user functionality and interface devices? A. The system management functionality of the AI environment is [physically/ logically] separated from the user functionality. This is done using [tools/ policies/ techniques].	Q. How is system management functionality of the AI platform separated from user functionality? A. The system management functionality of the AI environment is [physically / logically] separated from the user functionality. This is done using [tools/ policies/ techniques].		
SC-03-00	Q. How are security functions of the AI environment isolated from non-security functions (regular user functions and management functions)? A. Security functions of the AI environment are [physically/ logically] isolated from other functions within the AI environment using [techniques/ policies/ tools]	Q. How are security functions of the AI platform isolated from non-security functions (regular user functions and management functions)? A. Security functions of the AI platform are [physically/ logically] isolated from other functions within the AI environment using [techniques/ policies/ tools]		

Control ID	Environment (infrastructure, network)	AI Platform (AI components, AI software)	AI Models (ML models, LLMs)	AI Data (training data, validation data)
SC-04-00	Q. Which measures are in place to prevent unintended information disclosures to unauthorized individuals or roles via shared system resources after they have been released back to the system? This includes encrypted data. A. The [measures] are in place to prevent unintended information transfer via shared system resources are [policies/ measures/ tools].	Q. What measures are in place to prevent the unauthorized disclosure of data from the shared resources of an AI platform? A. The [measures] taken to prevent the unauthorized disclosure of data through the AI platform are [policies], which are carried out using [tools].	Q. What measures are in place that limit the possibility of data exfiltration from systems that contain AI Models? A. The measures in place to mitigate the exfiltration of data relating to AI models are [measures/tools].	Q. What protection is implemented to prevent unauthorized and unintended information transfer via shared data systems concerning AI training data at rest? A. The protection mechanisms in use to protect disclosure of AI data at rest are [mechanisms/ policies] which are carried out using [tools].
SC-05-00	Q. What kind of mechanisms are used to prevent Denial of Service (DOS) attacks against the systems comprising of the AI environment? A. The protections implemented throughout the AI environment include [tools/devices] using [configuration]. Q. How have controls been employed in the AI environment to achieve the denial-of-service mitigations for each type of denial-of-service event? A. The controls that are used within the environment are [controls/policies]. Q. What controls have been employed within the AI environment to achieve denial-of-service mitigations for cost harvesting? A. [XYZ controls] have been employed within the AI environment to achieve denial-of-service mitigations for cost harvesting.	Q. What kind of mechanisms are used to prevent DOS attacks against the systems that host the AI platform? A. The protections implemented on the AI platform are [tools/devices] using [configuration]. Q. How have controls been employed on the AI platform to achieve denial-of-service (DOS) mitigations for each type of DOS event? A. The controls that are used within the environment are [controls/policies]. Q. What controls have been employed within the AI platform to achieve denial-of-service mitigations for cost harvesting? A. [XYZ controls] have been employed within the AI platform to achieve denial-of-service mitigations for cost harvesting.		
SC-06-00	Q. How is resource availability protected in AI environments to ensure proper prioritization? A. Resource availability is protected within the AI environment by allocating [resource amount] according to [priority levels/quotas/controls].	Q. How is resource availability protected for the AI platform? A. Resource availability is protected by the AI platform by allocating [resources] according to [priority/quotas/controls].		

Control ID	Environment (infrastructure, network)	AI Platform (AI components, AI software)	AI Models (ML models, LLMs)	AI Data (training data, validation data)
SC-07-00	Q. How are communications monitored and controlled at the externally managed interfaces to the AI environment; and at key internal managed interfaces within the AI environment? A. Communications are monitored using [tools/methods] and controlled using [tools/policies], from external managed interfaces and key internal interfaces within the AI environment. Q. How are subnetworks configured for publicly accessible elements of the AI environment to be separated from internal organizational networks? A. The subnetworks for publicly accessible systems in the environment are [physically/ logically] separated from internal organization networks. Q. How are external networks permitted to be connected to from within the AI environment? How is boundary protection established at these connection points? A. External networks are only allowed to be connected to from managed interfaces with boundary protections. Boundary protection devices consist of [devices].	Q. How are communications monitored and controlled at the externally managed interfaces to the AI platform? A. Communications are monitored using [tools/methods] and controlled using [tools/policies], from externally managed interfaces connected to the AI platform. Q. How are subnetworks configured for publicly accessible elements of the AI platform to be separated from internal organizational networks? A. The subnetworks for publicly accessible elements of the AI platform are [physically/ logically] separated from internal organization networks. Q. How does the AI platform handle outgoing external network connections? How is boundary protection established at these connection points? A. External networks are only allowed to be connected to from managed interfaces with boundary protections. Boundary protection devices consist of [devices].		Q. How are communications with AI training data monitored and controlled at externally managed interfaces? A. Communications are monitored using [tools/methods] and controlled using [tools/policies], from externally managed interfaces.

Control ID	Environment (infrastructure, network)	AI Platform (AI components, AI software)	AI Models (ML models, LLMs)	AI Data (training data, validation data)
SC-08-00	Q. How is the confidentiality and integrity of transmitted information protected to/from/within the AI environment, including internal and external networks, and all system components capable of transmitting information? A. The [physical and/or logical] means to protect the confidentiality and integrity of all transmitted information through AI environment are [tools, techniques, policies]. Q. How is the confidentiality and integrity of information, in transit, protected when using LLM plugins? A. CI in transit is protected via [methods].	Q. How is the AI platform designed to protect the confidentiality and integrity of transmitted information? A. The AI platform protects the confidentiality and integrity of transmitted information by using [tools, techniques, policies].	Q. How is the confidentiality and integrity of transmitted models assured? A. The confidentiality and integrity of transmitted models is assured by [tools, techniques, policies]. Q. How is cryptography used to prevent unauthorized disclosure of AI models and detect changes to models during data transmissions? A. Cryptography is used to protect AI models from disclosure and change by [methods.]	Q. How is the confidentiality and integrity of transmitted information protected within the AI training data or data storage systems during transmission? A. The confidentiality and integrity of AI data is protected during transmission because of [tools, techniques, policies] used within the AI training data and/or data storage systems. Q. How is cryptography used to prevent unauthorized disclosure of AI data and detect changes to data during transmission? A. Cryptography is used to protect AI data from disclosure and change by [methods.]
SC-10-00	Q. What is the policy for terminating network connections in the AI environment associated with communication sessions.? A. The network connection is to be terminated [at the end of the session or after the org-defined period of inactivity] to internal and external networks from the AI environment.	Q. What is the policy for terminating communication sessions on the AI platform? A. The network connection is to be terminated [at the end of the session or after the organizationally defined period of inactivity] to internal and external networks from the AI platform.		Q. How are communication sessions with AI data terminated? A. The network connection accessing AI data internally or externally is terminated [at the end of the session or after the organization-defined period of inactivity].
SC-12-00	Q. How are cryptographic keys established and managed within the AI environment in accordance with organization policy- containing standards for key generation, distribution, storage, access, and destruction? A. Cryptographic key management is an [automated/manual] procedure. Keys are generated, stored, accessed, and destroyed through [organization defined requirements], using managed trust stores from only approved trust anchors.		Q. How are cryptographic keys established to protect the confidentiality and integrity of AI models in storage in accordance with the organization-defined requirements for key generation, distribution, storage, access, and destruction? A. Cryptographic key management is an [automated/manual] procedure. Keys are generated, stored, accessed, and destroyed through [organization defined requirements], using managed trust stores from only approved trust anchors.	Q. How are cryptographic keys established and managed in the storage, encryption, and verification of integrity of AI data, in accordance with organization-defined requirements for key generation, distribution, storage, access, and destruction? A. Cryptographic key management is an [automated/manual] procedure. Keys are generated, stored, accessed, and destroyed through [organization defined requirements], using managed trust stores from only approved trust anchors.

Control ID	Environment (infrastructure, network)	AI Platform (AI components, AI software)	AI Models (ML models, LLMs)	AI Data (training data, validation data)
SC-13-00			Q. How is cryptography being used to protect the confidentiality and integrity of AI models? A. Cryptography is being used by the AI model to protect its confidentiality through [methods] and integrity using [methods].	Q. How is cryptography being used to protect the confidentiality and integrity of AI data? A. Cryptography is being used in the AI data to protect its confidentiality through [methods] and integrity using [methods].
SC-15-00	Q. Is remote activation of collaborative computing devices and applications prohibited, and what are the exceptions? A. Yes, remote activation is prohibited, with the following [exceptions]. Q. What is the explicit indication of use provided to users physically present at the collaborative computing devices and applications within the AI environment when they are activated? A. The explicit indication of use is [indication].	Q. Is remote activation of collaborative AI powered applications prohibited, and what are the exceptions? A. Yes, remote activation is prohibited, with the following [exceptions]. Q. What is the explicit indication of use provided to users physically present at the AI powered applications when they are activated? A. The explicit indication of use is [indication].		
SC-17-00	Q. How are public key infrastructure (PKI) certificates issued for the AI environment? A. The [certificate policy or approved service provider] provides PKI for the AI environment. Only approved trust anchors are included in managed [trust stores or certificate stores].	Q. How are PKI certificates issued for the AI platform? A. The [certificate policy or approved service provider] provides PKI for the AI platform. Only approved trust anchors are included in managed [trust stores or certificate stores].		Q. How are PKI certificates issued for AI data? A. The [certificate policy or approved service provider] provides PKI for the AI data. Only approved trust anchors are included in managed [trust stores or certificate stores].

Control ID	Environment (infrastructure, network)	AI Platform (AI components, AI software)	AI Models (ML models, LLMs)	AI Data (training data, validation data)
SC-18-00	Q. Within the AI environment, how are acceptable and unacceptable mobile code and mobile code technologies defined? A. The policies defining acceptable/ unacceptable uses of mobile code are [policies]. Q. How is the use of mobile code within the AI environment authorized, monitored, and controlled? A. The use of mobile code in the AI environment is authorized, monitored, and controlled using [tools] and [policies].	Q. On an AI platform, how are acceptable and unacceptable mobile code and mobile code technologies defined? A. The policies defining acceptable/ unacceptable uses of mobile code are [policies]. Q. How is the use of mobile code within the AI platform authorized, monitored, and controlled? A. The use of mobile code on the AI platform is authorized, monitored, and controlled using [tools] and [policies].		
SC-23-00	Q. How is confidence in data validity being established during communication sessions throughout the AI environment? How are users able to verify the authenticity of identities with parties at either end of a communication session? What are the protections against man-in-the-middle (MITM) attacks, session hijacking, and false information injections. A. Users can be confident that data is legitimate during a communication session on the environment because of [protections]. Integrity of identity if validated because of [protections] and ensure protection against MITMs, session hijacking, and false data injection.	Q. How does the AI platform ensure the validity of outgoing data and incoming requests during a communication session? How can a user ensure they are speaking directly with the AI platform, with no alteration or interception. A. The AI platform protects the authenticity of all communication sessions using [methods] to validate identity and data of both ends of a communication session.		
SC-24-00	Q. How is failure in a known state implemented to prevent loss or damage to the environment? A. Failing to a known state is accomplished by [means].	Q. How is system state information preserved to facilitate system restart and return to operational mode with minimal disruption? A. State information is preserved by [means].	Q. What are the organizational defined fail states defined for the AI model? A. The ODPs defined for failing to known states are [ODPs].	

Control ID	Environment (infrastructure, network)	AI Platform (AI components, AI software)	AI Models (ML models, LLMs)	AI Data (training data, validation data)
SC-28-00	Q. What measures are employed to protect the confidentiality and integrity of information at rest in the AI environment? How are disk drives, network storage devices, and databases protected from breach, and in the event of a breach, how is confidentiality maintained? A. The measures employed to protect information at rest are [measures]. Environment storage devices are protected from access using [tools] and [protocols] are used to protect the data from disclosure.	Q. How is AI component software protected at rest? A. AI component software is protected at rest by [means].	Q. What measures are employed to protect the confidentiality and integrity of the AI models? How are devices and systems containing AI models protected from breach? How is the integrity of AI models protected from alteration and unauthorized disclosure in the event of a breach? A. The measures employed to protect models' information at rest are [measures]. Storage devices containing models are protected from unauthorized access using [tools] and [protocols] are used to protect the data from disclosure. The integrity of the models is verified using [protocols].	Q. What measures are employed to protect the confidentiality and integrity of the AI data? How are devices and systems containing AI data protected from breach? How is the integrity of AI training data protected from unauthorized alteration? A. The measures employed to protect the AI training data at rest are [measures]. Storage devices containing data are protected from unauthorized access using [tools] and [protocols] are used to protect the data from disclosure in the event of a breach. The integrity of the data is verified using [protocols] to ensure it has not been tampered with or poisoned via a breach.
SC-37-00	Q. How are out-of-band channels protected to prevent unauthorized introduction of AI components, models, and data into the environment? A. Out-of-band channels prevent the unauthorized introduction of AI components, models, and data into the environment by [methods].	Q. Are authorized out-of-band channels enabled to ensure business continuity and availability of AI-enabled systems? A. The [authorized out-of-band channels] are enabled to ensure business continuity and availability of AI-enabled systems.		
SC-39-00	Q. How is each executing system process assigned a separate address space to maintain separate execution domains within the AI environment? A. Separate address space for the AI environment is established by [means].	Q. How is each executing system process assigned a separate address space to maintain separate execution domains within the AI platform? A. Separate address space for the AI platform is established by [means]. Q. How does the AI platform enforce process isolation for LLM plugins? A. The AI platform isolates plugins by [means].		

'Approved for Public Release; Distribution Unlimited. Public Release Case Number 25-1028.

Control ID	Environment (infrastructure, network)	AI Platform (AI components, AI software)	AI Models (ML models, LLMs)	AI Data (training data, validation data)
SI-02-00	Q. What is the protocol for flaw remediation upon detection of a system flaw, and is remediation incorporated in organization configuration management process? How is software and firmware tested for effectiveness and potential side effects before installation? What is the lag time between the release of a security relevant software/firmware update and the installation of the update? A. Upon identifying a system flaw using [method/tool], which is [integrated/ not integrated] within organization config management process, flaws are reported and sent for correction. Software/firmware updates concerning flaw remediation [are/are not] tested for effectiveness and potential side effects before installation. Security relevant software/firmware updates are installed within [period] and [do/ do not] comply with organization installation standards.	Q. What is the protocol for flaw remediation upon detection of a flaw concerning AI platform, and is remediation incorporated in organization configuration management process? How is the AI platform, and accompanying software and firmware tested for effectiveness and potential side effects before installation? What is the lag time between the release of a security relevant software/firmware update and the installation of the update? A. Upon identifying a system flaw using [method/tool], which is [integrated/ not integrated] within organization config management process, flaws are reported and sent for correction. Software/firmware updates concerning flaw remediation [are/are not] tested for effectiveness and potential side effects before installation. Security relevant software/firmware updates are installed within [period] and [do/ do not] comply with organization installation standards.		

SI-03-00	Q. Which [signature/non signature based] mechanisms are deployed at system entry and exit points to detect and remove malicious code? How often are these mechanisms updated with the latest releases of software, tools, policies, and configurations? A. The environment employs [signature/non signature] based detection across [all/some] entry and exit points. These mechanisms are capable of scanning [all/certain] types of files, [including/not including] compressed files and hidden code (steganography). These mechanisms are updated with latest [code signatures/ reputation-based technology/heuristics]. Q. Are protection mechanisms configured to perform periodic scans of the entire environment, and real time scans of external files as they are [downloaded, opened, or executed]? How are protection mechanisms (anti exploitation software) configured to operate? How are falsely positive detections and removals of code addressed concerning the impact on availability of the environment? A. Protection mechanisms perform real time scans on all files as they are [downloaded/ opened/ executed] before they are allowed to enter the environment. The entire environment is also scanned [periodically/piece mail] to detect malicious code that made it past real time protection mechanisms. Anti exploitation protection mechanisms prevent compromise by blocking malicious code from running, while quarantining the file/program, and sending an alert to the security team automatically upon detection. The potential impact of false detection and removal of benign	Q. Which [signature/non signature based] mechanisms are deployed at entry and exit points to the AI platform to detect and remove malicious code? How often are these mechanisms updated with the latest releases of software, tools, policies, and configurations? A. The AI platform employs [signature/non signature] based detection across [all/some] entry and exit points when processing data. These mechanisms are capable of scanning [all/certain] types of files, [including/not including] compressed files and hidden code (steganography). These mechanisms are updated with latest [code signatures/ reputation-based technology/heuristics]. Q. How are real-time scans of files performed as they are fed into the AI platform. How are protection mechanisms (anti exploitation software) configured to operate? A. Protection mechanisms perform real time scans on all files as they are imported into the AI platform, before they are allowed to be processed by the system. Periodic scans are performed on the AI platform to check for malicious code running on the platform. Anti exploitation protection mechanisms prevent compromise by blocking malicious code from being processed, while quarantining the file, and sending an alert to the security team automatically upon detection. The potential impact of false detection and removal of benign code on platform availability is addressed by [protocol]. Q. How is the AI platform robustness evaluated against adversarial attacks?	Q. Which [signature/non signature based] mechanisms are used to detect model compromise? How often are these mechanisms updated with the latest releases of software, tools, policies, and configurations? A. The system employs [signature/non signature] based detection mechanisms, which are capable of scanning [all/certain] types of files, [including/not including] compressed files and hidden code (steganography). These mechanisms are updated with latest [code signatures/ reputation-based technology/heuristics]. Q. How are protection mechanisms configured to perform [periodic] scans of the entire model, and real time scans of all files and code as they are incorporated into the model? How are protection mechanisms (anti exploitation software) configured to preserve the integrity of the model? How are falsely positive detections and removals of code addressed concerning the impact on availability of the AI model? A. Protection mechanisms perform real-time scans on all files before they are allowed to enter the model. The entire model is also scanned [periodically] to detect malicious code that made it past real time protection mechanisms and to account for new intelligence. Anti exploitation protection mechanisms prevent compromise by blocking malicious code from running within the model, while quarantining the file/program, and sending an alert to the security team automatically upon detection. The potential impact of false detection and removal of benign code on	Q. Which [signature/non signature based] mechanisms are deployed at storage devices to detect and remove malicious code? How often are these mechanisms updated with the latest releases of software, tools, policies, and configurations? A. The environment employs [signature/non signature] based detection across at entry points to storage devices. These mechanisms are capable of scanning [all/certain] types of files, [including/not including] compressed files and hidden code (steganography). These mechanisms are updated with latest [code signatures/ reputation-based technology/heuristics]. Q. How are protection mechanisms configured to perform periodic scans of the entire data storage architecture at rest, and real time scans of external files as they are downloaded? How are protection mechanisms (anti exploitation software) configured to operate within data storage? How are falsely positive detections and removals of code addressed concerning the impact on availability of the AI data? A. Protection mechanisms perform real-time scans on all files as they are downloaded and before they are allowed to enter the data storage system. The entire data storage is also scanned [periodically/piece mail] to detect malicious code that made it past real time protection mechanisms. Anti exploitation protection mechanisms prevent compromise by blocking malicious code from running, while quarantining the file/program, and sending an alert to the security team automatically upon detection.

Control ID	Environment (infrastructure, network)	AI Platform (AI components, AI software)	AI Models (ML models, LLMs)	AI Data (training data, validation data)
	code on system availability is addressed by [protocol].	A. Models are regularly evaluated for robustness against adversarial attacks by [methods]. Q. How is the system monitored for potential backdoors introduced into the AI platform during transfer learning? A. The system is monitored for potential backdoors introduced into the AI platform during transfer learning via [methods]. Q. In the AI platform, what malicious code mechanisms are implemented in the chat plugin to detect and eradicate malicious code? A. In the AI platform, [malicious code mechanisms] are implemented in the chat plugin to detect and eradicate malicious code. Q. What malicious code protection mechanisms are implemented in the AI platform to scan for indirect prompt injections? A. [malicious code protection mechanisms] are implemented in the AI platform to scan for indirect prompt injections. Q. What malicious code protection mechanisms are implemented in the AI platform to scan for direct prompt injections? A. [malicious code protection mechanisms] are implemented in the AI platform to scan for direct prompt injections. Q. What malicious code protection mechanisms are implemented in the AI platform to prevent malicious plugins from being used? A. The [procedures] are in place to ensure that plugins are safe.	model availability is addressed by [protocol]. Q. How is the AI model robustness evaluated against adversarial attacks? A. Models are regularly evaluated for robustness against adversarial attacks by [methods]. Q. How is the system monitored for potential backdoors introduced into the AI models during transfer learning? A. The system is monitored for potential backdoors introduced into the AI models during transfer learning via [methods].	The potential impact of false detection and removal of benign code on data availability and integrity is addressed by [protocol]. Q. How is the system monitored for potential backdoors introduced into the AI data during transfer learning? A. The system is monitored for potential backdoors introduced into the AI data during transfer learning via [methods]. Q. What malicious code protection mechanisms are implemented in the AI data to scan for indirect prompt injections? A. [malicious code protection mechanisms] are implemented in the AI data to scan for indirect prompt injections. Q. What malicious code protection mechanisms are implemented in the AI data to scan for direct prompt injections? A. [malicious code protection mechanisms] are implemented in the AI data to scan for direct prompt injections.

Control ID	Environment (infrastructure, network)	AI Platform (AI components, AI software)	AI Models (ML models, LLMs)	AI Data (training data, validation data)
SI-04-00	Q. What policies/ tools/ devices are used to monitor the environment for unauthorized system use, and IOCs (including the detection of unauthorized local, network, and remote connections)? What is the process for analyzing detected events and anomalies using collected data? A. The environment is monitored using [methods]. Events [are/are not] analyzed for collection of threat intelligence. Q. What strategy is in play to deploy monitoring devices throughout the system to collect [essential info], and which locations are selected as ad hoc locations for tracking specific transactions of interest. How is monitoring level adjusted when considering changes in risk to organization? A. Locations for deploying monitoring devices throughout the environment and ad hoc locations are chosen through [means] and collect [certain info]. Monitoring [is/is not] expanded in times of increased risk to [organization operations and assets/ individuals/ other orgs/ the nation].	Q. How are attacks to AI detected on the platform? A. The system detects attacks on the AI platform using [methods/tools]. Q. What types of AI-specific information is monitored? A. The types of AI-specific information monitored is [methods]. Q. To what roles are monitoring results of AI-specific information directed? A. The monitoring results of AI-specific information is directed to [ISSO, System Owner, and the Insider threat group]. Q. How does system monitoring conduct thorough data quality assessments for the AI platform before training AI models? A. System monitoring conducts data quality assessments with [methods]. Q. How does system monitoring detect and remove malicious or biased data injected during training with the AI platform? A. System monitoring detects and removes malicious or biased data injected during training by [methods]. Q. How does the system monitor and detect indirect prompt injections within the AI platform? A. The system monitors and detects indirect prompt injections via [methods] within the AI platform. Q. How does the system monitor and detect direct prompt injections within the AI platform? A. The system monitors and detects direct prompt injections via [methods] within the AI platform.	Q. How are attacks to AI detected on the platform? A. The system detects attacks on the AI platform using [methods/tools]. Q: How is poisoned data detected for the AI Model? How are the tools that poisoned the data detected? A: Develop a set of the human ground-truth testing data set to assess the functionality enabled by AI then compare and evaluate the test results, analyze the nature of the deviation from the expected results to determine the level of severity of functional defects, source of the defects, traces and scope of data poisoning, and report and alert the Security office of the detection of data poisoning.	Q. How does the system monitor and detect data poisoning, injection of false or misleading information within the training dataset, and modifying or deleting a portion existing datasets? A. The system detects data poisoning, injecting false or misleading information within the training dataset and modifying or deleting portions of existing datasets by [means]. Q. How does the system ensure that data was not pre-poisoned prior to acquisition? A. The system detects pre-poisoning through [methods]. Q. How does system monitoring conduct thorough data quality assessments for the AI data before training AI models? A. System monitoring conducts data quality assessments with [methods]. Q. How does system monitoring detect and remove malicious or biased data injected during training AI data? A. System monitoring detects and removes malicious or biased data injected during training by [methods]. Q. How does the system monitor and detect indirect prompt injections within the AI data? A. The system monitors and detects indirect prompt injections via [methods] within the AI data. Q. How does the system monitor and detect direct prompt injections within the AI data? A. The system monitors and detects direct prompt injections via [methods] within the AI data.

Control ID	Environment (infrastructure, network)	AI Platform (AI components, AI software)	AI Models (ML models, LLMs)	AI Data (training data, validation data)
SI-05-00	Q. What policies are in place for generating and distributing ongoing system security alerts, advisories, and directives? How does the organization distribute its own internal threat alerts? What is the speed of compliance with security directives? A. Security alerts, advisories, and directives are received from [source] on an ongoing basis. Internal alerts are also generated as needed as vulnerabilities are discovered within the environment. This information is disseminated to [personnel or roles/ elements/ external orgs]. The directives [are / are not] implemented within established time frames [or issuing organization is notified].	Q. What policies are in place for generating and distributing security alerts, advisories, and directives concerning threats to the AI platform? How does the organization distribute its own internal threat alerts? What is the speed of compliance with security directives? A. Security alerts, advisories, and directives are received from [source] on an ongoing basis. Internal alerts are also generated as needed using [tools] within the platform. This information is disseminated to [personnel or roles/ elements/ external orgs]. The directives [are / are not] implemented within established time frames [or issuing organization is notified].	Q. What policies are in place for generating and distributing security alerts, advisories, and directives concerning threats to the AI models? How does the organization distribute its own internal threat alerts? What is the speed of compliance with security directives? A. Security alerts, advisories, and directives are received from [source] on an ongoing basis. Internal alerts are also generated as needed using [tools] within the platform. This information is disseminated to [personnel or roles/ elements/ external orgs]. The directives [are / are not] implemented within established time frames [or issuing organization is notified].	Q. What policies are in place for generating and distributing security alerts, advisories, and directives concerning threats to the AI Data? How does the organization distribute its own internal threat alerts? What is the speed of compliance with security directives? A. Security alerts, advisories, and directives are received from [source] on an ongoing basis. Internal alerts are also generated as needed using [tools] within the platform. This information is disseminated to [personnel or roles/ elements/ external orgs]. The directives [are / are not] implemented within established time frames [or issuing organization is notified].
SI-07-00	Q. Which tools are in place to verify the integrity of software, firmware, and programs on the environment? What is the response plan when unauthorized changes are detected to the environment? A. The [tools] are performing integrity verification on the AI environment, which monitor [specific software/ firmware/programs]. Upon detecting unauthorized changes to software/ firmware/ programs/ component within the environment, [actions] are performed.	Q. Which tools are in place to verify the integrity of AI software and firmware on the AI platform? What is the response plan when unauthorized changes are detected to the platform? A. The [tools] are performing integrity verification on the AI platform, which monitor [software/ firmware/ tools]. Upon detecting unauthorized changes to the software/ firmware on the platform, [actions] are performed. Q. How are techniques such as adversarial training and robust optimization used to test the AI platform? A. Adversarial training and robust optimization are used via [methods] to test the AI platform.	Q. Which tools are in place to verify the integrity of AI models? What is the response plan when unauthorized changes are detected to the model? A. The [tools] performing integrity verification on the AI models, which monitor [specific elements/entire model] for unauthorized changes. Upon detecting an integrity violation to the model, [actions] are performed. Q. How are techniques such as adversarial training and robust optimization used to test the AI models? A. Adversarial training and robust optimization are used via [methods] to test the AI models.	Q. Which tools are in place to verify the integrity of AI data? What is the response plan when unauthorized changes are detected on the data? A. The [tools] performing integrity verification on the AI data, which monitor [training data/test data/data storage systems] for unauthorized changes. Upon detecting an integrity violation to the data, [actions] are performed. Q. How are techniques such as adversarial training and robust optimization used to test the AI data? A. Adversarial training and robust optimization are used via [methods] to test the AI data.

Control ID	Environment (infrastructure, network)	AI Platform (AI components, AI software)	AI Models (ML models, LLMs)	AI Data (training data, validation data)
SI-10-00		Q. How are AI Platforms validated to ensure that they have not been tampered with? A. Answer should include things like hashes and other ways to detect changes to the data. Q. What kind of input or prompt validation is performed prior to executing queries or taking any actions? A. The [validation checks] are performed on all input provided to the platform. Q. How are prompt filters updated and reviewed to prevent bypassing in the AI Platform? A. Prompt filters are regularly updated and reviewed through [methods]. Q. What information input validation does the AI platform contain to prevent indirect prompt injection? A. The AI platform contains information [input validation checks] to prevent indirect prompt injections. Q. What information input validation does the AI platform contain to prevent direct prompt injection? A. The AI platform uses information [input validation checks] to prevent direct prompt injections. Q. How is the input provided to LLM plugins validated prior to use? A. Input is validated by using the [libraries] prior to processing the input.	Q. How are AI Models and wights matrices validated to ensure that they have not been tampered with? A. Answer should include things like hashes and other ways to detect changes to the data. Q. What kind of input or prompt validation is performed prior to executing queries or taking any actions? A. The [validation checks] are performed on all input provided to AI models. Q. How are prompt filters updated and reviewed to prevent bypass in the AI models? A. Prompt filters are regularly updated and reviewed through [methods].	Q. How is the AI training data validated to ensure that it has not been tampered with? A. Answer should include things like hashes and other ways to detect changes to the data. Q. How are prompt filters updated and reviewed to prevent bypass in the AI data or training process? A. Prompt filters are regularly updated and reviewed through [methods]. Q. What information input validation are used to prevent indirect prompt injection? A. The [validation checks] are used to prevent indirect prompt injections. Q. What information input validation are used to prevent direct prompt injection? A. The [validation checks] are used to prevent indirect prompt injections.

Control ID	Environment (infrastructure, network)	AI Platform (AI components, AI software)	AI Models (ML models, LLMs)	AI Data (training data, validation data)
SI-11-00		Q. What is the behavior of error messages on the AI platform? A. Error messages are generated to provide necessary information for corrective actions without revealing exploitable information and messages are only revealed to [personnel].		
SI-16-00	Q. Which organization defined controls are implemented to protect system memory from unauthorized code execution? Are data-execution controls (if applicable) hardware or software enforced, and how are they combined with address space layout randomization within the environment to prevent writing backdoor executable code in prohibited memory locations? A. The system memory in the environment is protected from unauthorized code execution by using [organization defined controls]. These controls [include / don't include] hardware/software data execution prevention and address space layout randomization throughout the AI environment.	Q. Which organization defined controls are implemented to protect memory dedicated to AI platforms from unauthorized code execution? Are data-execution controls (if applicable) hardware or software enforced, and how are they combined with address space layout randomization on the platform's non-executable memory regions to prevent writing potentially backdoor executable code in prohibited memory locations? A. The AI platform memory is protected from unauthorized code execution by using [organization defined controls]. These controls [include/don't include] hardware/software data execution prevention and address space layout randomization on memory used for AI platforms.		
SI-20-00			Q. How are the AI models tainted to help determine whether the AI/ML models have been exfiltrated from the enterprise or improperly removed from the AI-enabled systems? A. The AI models are tainted by [methods].	Q. How are the AI models tainted to help determine whether the AI/ML models have been exfiltrated from the enterprise or improperly removed from the AI-enabled systems? A. The AI models are tainted by [methods].
SR-01-00		Q. How is the provenance of AI platform components assured for validity? A. The provenance of AI platform components is assured by [methods and assignment of organizationally defined parameters (ODPs)]. (Ref: SR-04)	Q. How is the provenance of AI models assured for validity? A. The provenance of AI models is assured by [methods and assignment of ODPs]. (Ref: SR-04)	Q. How is the provenance of AI datasets assured for validity? A. The provenance of AI datasets is assured by [methods and assignment of ODPs]. (Ref: SR-04)

Control ID	Environment (infrastructure, network)	AI Platform (AI components, AI software)	AI Models (ML models, LLMs)	AI Data (training data, validation data)
SR-02-00		Q. How does the Supply Chain Risk Management Plan implement bias-awareness training and post processing techniques for the AI platform? A. The Supply Chain Risk Management Plan includes [bias-awareness training and post processing techniques].	Q. For models that are not maintained/ developed internally what is the process to ensure that changes to the model do not negatively affect the system? A. For these models, [processes] are used to review changes before they are moved into the production environment. Q. How does the Supply Chain Risk Management Plan implement bias-awareness training and post processing techniques for the AI models? A. The Supply Chain Risk Management Plan includes [bias-awareness training and post processing techniques].	Q. For AI data that is not maintained/developed internally what is the process to ensure that changes to the data do not, negatively, affect the system? A. For AI data, the [processes] are used to review changes before they are moved into the production environment. Q. How does the Supply Chain Risk Management Plan implement bias-awareness training and post processing techniques for the AI data and training? A. The Supply Chain Risk Management Plan includes [bias-awareness training and post processing techniques].
SR-03-00	Q. How is the environment protected against the introduction of unvetted public and open-source AI models, software, and tools? A. The environment is protected against the introduction of unvetted public and open-source AI models, software, and tools by [methods]	Q. How is the AI platform protected against the introduction of unvetted public and open-source AI models, software, and tools? A. The environment is protected against the introduction of unvetted public and open-source AI models, software, and tools by [methods]. Q. How are weakness in the AI platform identified and mitigated? A. Weakness are identified via [methods]. Once a weakness is identified we research available patches, test them in the development and test environments first to ensure that there are no problems with the current baseline, after they have been thoroughly tested, they are applied to the production environment.	Q. How is the chain of custody for the AI Model supply chain maintained and tracked? A. The chain of custody for AI Models is maintained by [methods].	Q. How is the chain of custody for the AI dataset supply chain maintained and tracked? A. The chain of custody for AI datasets is maintained and tracked by [methods].
SR-04-00		Q. How is the provenance of AI platform components assured for validity? A. The provenance of AI platform components is assured by [methods and assignment of ODPs].	Q. How is the provenance of AI models assured for validity? A. The provenance of AI models is assured by [methods and assignment of ODPs].	

Control ID	Environment (infrastructure, network)	AI Platform (AI components, AI software)	AI Models (ML models, LLMs)	AI Data (training data, validation data)
SR-05-00	Q. What acquisition strategies, contract tools, and procurement methods are employed to protect against, identify, and mitigate supply chain risks in the AI environment? Which tools are techniques are employed in the environment to mitigate unauthorized production, theft, tampering, insertion of counterfeits, insertion of malicious software or backdoors, and poor development practices throughout the development life cycle. A. The strategies, tools, and procurement methods used to protect against supply chain risks are [XYZ]. Supply chain threats are mitigated in the environment by using [tools] to identify, monitor, and protect against risks.	Q. What acquisition strategies, contract tools, and procurement methods are employed to protect against, identify, and mitigate supply chain risks with AI platforms? Which tools and procedures are established to mitigate unauthorized production, theft, tampering, insertion of counterfeits, insertion of malicious software or backdoors, and poor development practices throughout the development life cycle of any AI platform. How is the organization ensuring AI developers follow the maximum level of supply chain integrity controls? A. The [strategies, tools, and procurement methods] are used to protect against supply chain risks within the AI platform. Organization uses strict assessment and verification of all AI software produced and employs [controls] throughout the entire supply chain. [Tools and techniques] are used to protect the integrity of the development process, providing protection for unauthorized production, theft, tampering, insertion of counterfeits, insertion of malicious software or backdoors, and poor development practices throughout the system development life cycle. Transparency into security and privacy practices [is/is not] promoted by the organization and implementing controls [is/is not] incentivized.		
SR-06-00		Q. What is the process to assess and review the supply chain-related risks associated with suppliers or contractors of the AI platform? A. The [processes] are used to review the suppliers or contractors of the AI platform.	Q. What is the process to assess and review the supply chain-related risks associated with suppliers or contractors of the AI models? A. The [processes] are used to review the suppliers or contractors of the AI models.	Q. What is the process to assess and review the supply chain-related risks associated with suppliers or contractors of the AI data? A. The [processes] are used to review the suppliers or contractors of the AI data.

Control ID	Environment (infrastructure, network)	AI Platform (AI components, AI software)	AI Models (ML models, LLMs)	AI Data (training data, validation data)
SR-08-00		Q. What agreements and procedures are in place with supply chain entities for the notification of compromises and potential compromises in the supply chain that can potentially adversely affect the AI platform? A. We have the [agreements] with the developers/vendors to ensure that we are promptly notified in these cases.	Q. What agreements and procedures are in place with supply chain entities for the notification of compromises and potential compromises in the supply chain that can potentially adversely affect the AI models? A. We have the [agreements] with the developers/vendors to ensure that we are promptly notified in these cases.	Q. What agreements and procedures are in place with supply chain entities for the notification of compromises and potential compromises in the supply chain that can potentially adversely affect the AI data? A. We have the [agreements] with the developers/vendors to ensure that we are promptly notified in these cases.
SR-09-00	Q. How is tamper protection provided for the components within the AI environment? What means of tamper protection is employed to protect these components during distribution and use? A. Tamper protection is provided for the AI environment and accompanying services by [methods]. Strong identification [is/ is not] used in conjunction with tamper [resistance/ detection].	Q. How is tamper protection provided for the AI system, components, and services? What means of tamper protection are employed to protect these systems during distribution and use? A. Tamper protection is provided for the AI system, components, and services by [methods]. Strong identification [is/ is not] used in combination with tamper [resistance/detection].		
SR-11-00		Q. How is assurance given that AI system components are not counterfeit? A. Assurance that AI system components are not counterfeit is given by [means].		