

ATTACHMENT A - INFORMATION TECHNOLOGY SECURITY MATRIX

VERSION 112024 REV. A

H.R. 5515

In accordance with US House of Representatives H.R. 5515 “National Defense Authorization Act for Fiscal Year 2021” House Bill, the Solution shall not utilize products or services from the manufacturers listed therein. [DOD Releases List of People's Republic of China \(PRC\) Military Companies in Accordance With Section 1260H of the National Defense Authorization Act for Fiscal Year 2021 > U.S. Department of Defense > Releases](#)

Use of Miami-Dade County Data and Systems:

1. **Access Control:** Miami-Dade County (MDC) employees, system users, contractors or those operating on their behalf are prohibited from incorporating or using AI-enabled services in such a way that Miami-Dade County data is uploaded or made available for data mining or usage. Uploading, copying, sharing, or transmitting any sensitive Miami-Dade created or managed data via methods or software not explicitly allowed are prohibited. This includes any PCI, PII, HIPAA, CJIS or other data that is created or managed by or on behalf of Miami-Dade County. Access controls are to be guided by the Miami-Dade County Enterprise Security Policy. The MDC Enterprise Security Policy is available to responsive bidders or upon request approved by the MDC Enterprise Security Office.
2. **Data Protection:** All data processed by Cloud-based or AI-enabled technologies must be protected from unauthorized access, theft, and misuse. Data must be encrypted in transit and at rest, and access controls should be in place to ensure that only authorized users can access the data. Data should be stored securely, and backups must be kept in a secure location. Usage of said data by the Cloud or AI provider must be communicated and agreed to, with consideration to transparency and with human oversight of use and potential abuse or misuse.
3. **Monitoring:** Any Cloud-based or AI-enabled technologies must be monitored for unusual activity or unauthorized access. Logs and alerts should be reviewed regularly, and security analytics should be used to identify potential threats or hallucinations.
4. **Vulnerability Management:** Any Cloud-based or AI-enabled technologies must be regularly assessed for vulnerabilities and weaknesses. Regular vulnerability scans and penetration testing must be conducted, and security assessments must be performed to identify areas of improvement.
5. **Incident Response:** Abuse or misuse to the extent that it endangers the security or privacy of Miami-Dade County citizens, users, data, personnel, or facilities must be reported according to the Miami-Dade County Enterprise Security Office Incident Response Plan.
6. **Training and Awareness:** All employees must receive training on the secure use of any Cloud-based or AI-enabled technologies. This should include best practices for data protection, access controls, and incident response.
7. **Compliance:** Any Cloud-based or AI-enabled technologies must be compliant with relevant laws and regulations, such as GDPR, HIPAA, and CCPA as well as compliant with Miami-Dade County Security Policy and the overall policies and procedures of Miami-Dade County. Regular audits should be conducted to ensure compliance.
8. **Risk Management:** A risk management program should be in place to identify and mitigate risks associated with the use of any Cloud-based or AI-enabled technologies. Risks should be regularly assessed, and appropriate controls should be put in place to mitigate those risks.
9. **Coordinated Vulnerability Disclosure:** Miami-Dade County follows a vulnerability disclosure model in which a vulnerability or an issue is disclosed to the public only after the responsible parties have been allowed sufficient time to patch or remedy the vulnerability or issue.

Instructions

- **Purpose:** This security matrix is designed to assess the security controls implemented by external vendors and contractors.
 - **Instructions:** This form should be completed by someone who is familiar with the proposed system and can answer technical security questions such as a Product Manager, CISO, CTO, CIO. Please save the completed file to include the name of the product and return the completed matrix in a **machine-readable format (e.g., Word or PDF)**.
 - For each functionality listed below, please select the code that best corresponds to your response and enter it in the **'Meet (Y/C/M/N)' column**. Provide detailed explanations or comments in the 'Detailed Explanation' column to clarify how the functionality is addressed. Provide diagrams and additional documentation when you return the completed security matrix.
 - **Response Codes:**
 - **Y – Fully met without configuration or modification.**
 - **C – Met via configuration (without changing base source code).**
 - **M – Met via modification of the base source code.**
 - **N – Not met. If an alternative compensating control is being proposed, please provide a detailed explanation. A blank or "N/A" response will be interpreted as "N".**
-

Vendor Information

- **Vendor Name:**
- **Contact Person:**
- **Title:**
- **Email:**
- **Phone Number:**

Security Matrix

A. Data Classification and Protection

Functionality Number	Functionality	Meet (Y/C/M/N)	Detailed Explanation	References
1	Type of Data Processed: Indicate all types of data your solution processes. Remove any that do not apply: - PII (Personally Identifiable Information) - PCI (Payment Card Industry) - PHI (Protected Health Information) - Critical Infrastructure - SCADA / ICS / OT - HR (Human Resources) - CJIS (Criminal Justice Information Services) - HIPAA - Financial Records - Other (please specify)			NIST CSF ID.AM-5; ISO 27001 A.8
2	Compliance and Risk Assessments: Has a SOC 2 Type II or other risk assessment been performed within the last 12 months? Please provide the most recent report.			NIST CSF ID.GV-1; SOC 2, ISO 27001

B. Risk Assessments and Compliance

Functionality Number	Functionality	Meet (Y/C/M/N)	Detailed Explanation	References
3	Compliance Certifications: Does the solution comply with any of the following standards? Please check all that apply and provide supporting documentation. - ISO/IEC 27001 - PCI DSS v4.0.1 - HIPAA - StateRAMP / FedRAMP - Other (please specify)			NIST CSF ID.GV-2; ISO 27001; StateRAMP; FedRAMP, PCI 4.0.1

C. Identity and Access Management

Functionality Number	Functionality	Meet (Y/C/M/N)	Detailed Explanation	References
4	Unique User Identification: The solution uniquely identifies each user.			NIST CSF PR.AC-1; CIS Control 6.2
5	Integration with Directory Services: The solution integrates with Microsoft Active Directory or Azure Active Directory (EntraID) for user authentication of internal users using protocols such as SAML, OAuth 2.0, or OpenID Connect.			NIST CSF PR.AC-1; CIS Control 6.1
6	Principle of Least Privilege (Operating Systems): The solution can be installed and maintained in accordance with the principle of least privilege for operating systems.			NIST CSF PR.AC-6; CIS Control 4
7	Principle of Least Privilege (Database Systems): The solution can be installed and maintained in accordance with the principle of least privilege for database systems.			NIST CSF PR.AC-6; CIS Control 4
8	Unique Process Identification: The solution uniquely identifies each process (system, service, Managed Service Accounts).			NIST CSF PR.AC-4; CIS Control 4
9	Scheduled Password Rotation: The solution supports scheduled password rotation of process accounts.			NIST CSF PR.AC-5; CIS Control 6.1
10	Disable or Rename Default Accounts: Default system accounts can be disabled or renamed (e.g., administrator/admin, guest).			NIST CSF PR.AC-1; CIS Control 5

Functionality Number	Functionality	Meet (Y/C/M/N)	Detailed Explanation	References
11	Inactive Account Management: Accounts are automatically disabled after a configurable period of inactivity (e.g., 90 days).			NIST CSF PR.AC-4; CIS Control 16.11
12	Password Authentication: The solution utilizes account passwords for authentication and supports passphrase best practices.			NIST CSF PR.AC-1; CIS Control 6
13	Password Complexity Requirements: User password complexity is configurable to allow for a minimum of 14 characters comprised of upper and lower-case letters, numbers, and special characters. System Accounts require complex passwords with a minimum of 25 characters and must be changed every 180 days. Use of Group Managed Service Accounts (gMSA) is strongly recommended.			NIST CSF PR.AC-1; CIS Control 6.3
14	Password Suppression: Passwords are suppressed (not echoed back) when entered by users.			NIST CSF PR.AC-1; CIS Control 6.5
15	Multi-Factor Authentication (MFA): The solution supports MFA for user authentication. Phishing Resistant Authentication is strongly recommended.			NIST CSF PR.AC-7; CIS Control 6.8
16	Encryption of Credentials in Transit: User login credentials are encrypted during transmission with a minimum of AES 256-bit encryption.			NIST CSF PR.DS-2; CIS Control 3.1
17	Password History and Reuse: The solution supports password history			NIST CSF PR.AC-1;

Functionality Number	Functionality	Meet (Y/C/M/N)	Detailed Explanation	References
	functionality to prevent reuse of a configurable number of prior passwords (minimum of 10).			CIS Control 6.4
18	Administrative Password Aging: The solution supports administrative password aging of 30 days.			NIST CSF PR.AC-1; CIS Control 6.3
19	Password Reset Capability: Administrative accounts have the capability of resetting passwords.			NIST CSF PR.AC-1; CIS Control 6
20	Self-Service Password Reset with Challenge Questions: The solution provides user self-service password reset functionality utilizing challenge-response authentication.			NIST CSF PR.AC-1; CIS Control 6.6
21	Challenge Question Security: Self-service challenge responses are comprised of at least 8 questions, with responses stored securely using AES 256-bit encryption.			NIST CSF PR.AC-1; CIS Control 6.6
22	Configurable Login Attempt Limits: The solution supports limiting unsuccessful login attempts to 5 before locking out or disabling the account.			NIST CSF PR.AC-7; CIS Control 16.7
23	Concurrent Session Control: The solution supports limiting concurrent user sessions to 1 by default; administrators can configure the number.			NIST CSF PR.AC-7; CIS Control 16.9
24	Account Lockout/Disable Capability: Administrators can lock or disable accounts whenever necessary.			NIST CSF PR.AC-4;

Functionality Number	Functionality	Meet (Y/C/M/N)	Detailed Explanation	References
				CIS Control 16.4
25	Pre-Login Banner: The solution can display a customizable pre-login warning banner stating that unauthorized access is prohibited.			NIST CSF PR.PT-2; CIS Control 16.1
26	Role-Based Access Control (RBAC): The solution supports managing users based on group membership and assigning/revoking specific privileges.			NIST CSF PR.AC-4; CIS Control 5
27	User Rights and Privileges Reporting: Tools and reports are available to enumerate user rights, group membership, access permissions, or user profiles.			NIST CSF PR.DS-6; CIS Control 4.4
28	Account Password Encryption in Storage: System Accounts, Passwords, Certificates, Keys, and other secrets are stored hashed and salted using strong cryptographic algorithms (e.g., SHA-256 with salt).			NIST CSF PR.DS-1; CIS Control 14.4

D. Audit Logging and Monitoring

Functionality Number	Functionality	Meet (Y/C/M/N)	Detailed Explanation	References
29	Audit Logging Capability: The solution captures audit logs of successful and unsuccessful logins, records viewed, printed, added, deleted, or modified, and retains logs for at least 5 years plus current.			NIST CSF DE.AE-3; CIS Control 8
30	Audit Log Details: Logs capture date and time, user account, source IP address, event details, and success or failure of the event.			NIST CSF DE.AE-3; CIS Control 8
31	Audit Mechanism Protection: Administrators cannot disable the audit mechanism.			NIST CSF PR.PT-1; CIS Control 8.8
32	Audit Log Integrity: Audit logs are protected from unauthorized access and alteration (e.g., sent to a SIEM in addition to local storage).			NIST CSF PR.PT-1; CIS Control 8.5
33	Audit Log Tamper Prevention: Users and administrators are prevented from modifying, deleting, or adding log entries.			NIST CSF PR.PT-1; CIS Control 8.5
34	Intrusion Detection and Prevention: The solution is protected using Intrusion Detection and Prevention Systems (IDS/IPS).			NIST CSF DE.CM-1; CIS Control 9
35	Protection Against DDoS Attacks: The solution is protected against Distributed Denial of Service (DDoS) attacks.			NIST CSF PR.DS-5; CIS Control 9
36	Security Event Notifications: The solution generates outbound alerts and notifications. Explain the data contained in these messages (e.g.,			NIST CSF DE.DP-5; CIS Control 8.7



Functionality Number	Functionality	Meet (Y/C/M/N)	Detailed Explanation	References
	email alerts, automated reports, SNMP v.3 traps).			

E. Software and Configuration Management

Functionality Number	Functionality	Meet (Y/C/M/N)	Detailed Explanation	References
37	Microsoft Enterprise Access Model Compliance: The solution can be installed and maintained according to the Microsoft Enterprise Access Model .			NIST CSF PR.IP-1; CIS Control 4
38	Software Version Control: The solution prevents outdated software versions from accessing the Database Management System (DBMS).			NIST CSF PR.IP-1; CIS Control 2.3
39	Patch Management: The solution is regularly patched with appropriate security patches within specified timeframes: - Critical patches: within 14 days of release - High patches: within 30 days - Medium and Low patches: within 90 days			NIST CSF PR.IP-12; CIS Control 7
40	Vulnerability Management: Regular vulnerability scans are performed (e.g., monthly) using tools like Nessus or Qualys. Reports are shared upon request.			NIST CSF PR.IP-12; CIS Control 7
41	Application Security Testing: Regular application vulnerability scans are conducted using tools like WebInspect, Veracode, or AppScan. Dynamic and Static Application scans are preferred.			NIST CSF PR.IP-12; CIS Control 18
42	Change Control Processes: Application vulnerability scanning (e.g., PCI DSS, OWASP Top 10)			NIST CSF PR.IP-3; CIS Control 6.1



Functionality Number	Functionality	Meet (Y/C/M/N)	Detailed Explanation	References
	is performed prior to production migration of changes. Medium, High, and Critical vulnerabilities are remediated before migration. Reports are shared upon request.			

F. Data Encryption and Transmission

Functionality Number	Functionality	Meet (Y/C/M/N)	Detailed Explanation	References
43	Data Encryption in Transit: Sensitive data is encrypted during transmission over the network using a minimum of TLS 1.2 with AES 256-bit encryption.			NIST CSF PR.DS-2; CIS Control 3.11
44	Data Encryption at Rest: Sensitive information is encrypted while in storage using a minimum of AES 256-bit encryption.			NIST CSF PR.DS-1; CIS Control 14
45	Encryption over External Networks: Sensitive information is encrypted for transmission over external networks using a minimum of AES 256-bit encryption.			NIST CSF PR.DS-2; CIS Control 3.11

G. Cloud Hosting and Infrastructure Security

Functionality Number	Functionality	Meet (Y/C/M/N)	Detailed Explanation	References
46	Data Center Compliance: If cloud-hosted, the solution is hosted in an audited data center complying with ISO/IEC 27001, SOC 2 Type II, StateRAMP, or FedRAMP standards. Provide the latest audit report.			NIST CSF PR.AC-5; StateRAMP; FedRAMP
47	Employee Access Controls: Controls prohibit hosting employees or third-party personnel from accessing, viewing, or modifying customer confidential data. Describe controls used, including encryption and key storage mechanisms.			NIST CSF PR.AC-5; CIS Control 14

Functionality Number	Functionality	Meet (Y/C/M/N)	Detailed Explanation	References
48	High Availability and Failover: The solution is highly available with active-active or active-passive failover between geographically diverse data centers.			NIST CSF PR.DS-4; CIS Control 12
49	Data Residency: System and data are physically located within the Continental United States.			NIST CSF PR.DS-5
50	Network Accessibility: System is accessible from the County's network and proxy infrastructure.			NIST CSF PR.AC-3
51	Session Encryption: All sessions are encrypted from initiation to termination using validated encryption ciphers (TLS 1.2 or higher).			NIST CSF PR.DS-2; CIS Control 3.11
52	Regular Vulnerability Scanning: Monthly vulnerability scans are performed using tools like Nessus, Tenable, or Qualys. Reports will be shared with the County if requested.			NIST CSF PR.IP-12; CIS Control 7
53	API Security: APIs use API key security (X-API-Key) or demonstrate alternate security controls.			NIST CSF PR.AC-1; CIS Control 14.8

H. Software Integrity and Secure Development

Functionality Number	Functionality	Meet (Y/C/M/N)	Detailed Explanation	References
54	Prevent Changes to Records: Users, developers, DBAs, or administrators cannot alter posted,			NIST CSF PR.IP-4; CIS Control 5



Functionality Number	Functionality	Meet (Y/C/M/N)	Detailed Explanation	References
	completed, or closed transaction records.			
55	Rollback Processes: Rollback processes are incorporated into the database for all critical transactions.			NIST CSF PR.IP-4; CIS Control 10.5
56	Outdated Software Access Prevention: The solution prevents outdated software versions from accessing the DBMS.			NIST CSF PR.IP-1; CIS Control 2.3

I. Artificial Intelligence (AI) and Machine Learning (ML) Controls

- Note:** This section addresses security controls specific to systems utilizing Artificial Intelligence (AI) and Machine Learning (ML). These controls ensure the trustworthy, secure, and ethical use of AI/ML technologies. Please refer to NIST.AI.600-1.pdf for detailed guidance.

Functionality Number	Functionality	Meet (Y/C/M/N)	Detailed Explanation	References
57	AI Governance and Oversight: The organization has established governance structures and policies for AI/ML system development and deployment, including defined roles and responsibilities.			NIST.AI.600-1.pdf; NIST AI RMF GOV
58	AI Risk Management Framework Application: The organization applies a risk management framework specific to AI/ML systems to identify, assess, and mitigate risks throughout the AI lifecycle.			NIST.AI.600-1.pdf; NIST AI RMF MAP
59	Data Quality and Integrity for AI/ML: Data used for training and testing AI/ML models is assessed for quality, relevance, and potential biases. Processes ensure data integrity and accuracy.			NIST.AI.600-1.pdf; NIST AI RMF MEASURE
60	Model Transparency and Explainability: AI/ML models are designed to be interpretable, with mechanisms to explain model decisions to stakeholders as appropriate.			NIST.AI.600-1.pdf; NIST AI RMF MANAGE
61	Security of AI/ML Systems: The AI/ML systems are protected against adversarial attacks (e.g., data poisoning, model inversion). Security controls safeguard AI assets and processes.			NIST.AI.600-1.pdf; NIST AI RMF SECURE

Functionality Number	Functionality	Meet (Y/C/M/N)	Detailed Explanation	References
62	Privacy Protection in AI/ML: Measures protect personal and sensitive information used in AI/ML systems, including compliance with data protection regulations and techniques like differential privacy.			NIST.AI.600-1.pdf; NIST AI RMF PROTECT
63	Fairness and Bias Mitigation: The organization identifies and mitigates biases in AI/ML models to promote fairness and prevent discrimination against any group.			NIST.AI.600-1.pdf; NIST AI RMF MEASURE
64	Monitoring and Maintenance of AI/ML Systems: Continuous monitoring detects performance degradation, biases, or security incidents in AI/ML systems, with processes for model updates.			NIST.AI.600-1.pdf; NIST AI RMF MANAGE
65	Ethical Considerations and Compliance: The organization adheres to ethical guidelines and legal requirements related to AI/ML, including transparency and accountability.			NIST.AI.600-1.pdf; NIST AI RMF GOV
66	Third-Party AI Components Management: If using third-party AI/ML components or services, the organization ensures they meet the same security and ethical standards, including due diligence.			NIST.AI.600-1.pdf; NIST AI RMF GOV
67	Incident Response for AI/ML Systems: The organization has incident response plans that include scenarios specific to AI/ML systems, such as model failures or adversarial attacks.			NIST.AI.600-1.pdf; NIST AI RMF RESPOND



Functionality Number	Functionality	Meet (Y/C/M/N)	Detailed Explanation	References
68	Documentation and Reporting of AI/ML Models: Comprehensive documentation of AI/ML models, including design decisions, training data, and testing results, is maintained and available for review.			NIST.AI.600-1.pdf; NIST AI RMF GOV

J. Software Bill of Materials (SBOM)

- **AGPL POLICY WARNING:** Code licensed under the GNU Affero General Public License (AGPL) **MUST NOT** be used at Miami-Dade County.

Functionality Number	Functionality	Meet (Y/C/M/N)	Detailed Explanation	References
69	SBOM Creation and Maintenance: An SBOM must be created and maintained for all software projects, listing all third-party libraries and their associated metadata.			NIST SP 800-161; CIS Control 2.3
70	SBOM Submission Formats: SBOMs must be submitted in CycloneDX or SPDX formats. If these formats are unavailable, a fillable form template must be used to capture the required information. At a minimum, the following details must be documented for each third-party library: Software Component or Library Name, Author, Version, Last Updated Date, Website, and License.			NIST SP 800-161; CIS Control 2.3
71	Regular SBOM Updates and Reviews: The SBOM must be updated and reviewed regularly to ensure accuracy and completeness.			NIST SP 800-161; CIS Control 2.3
72	Licensing Compliance Review: A licensing compliance review must be conducted, and the results must be signed by the developer's management before any third-party library is used in production.			NIST CSF ID.SC-3; ISO 27001 A.18.1.3

General Comments

- Please provide any additional information or clarifications below:

Notes:

- **Applicability of Sections:** Ensure you complete all sections relevant to your solution, including the new Software Bill of Materials (SBOM) section.
- **AGPL Policy Compliance:** Under no circumstances should code licensed under the **GNU Affero General Public License (AGPL)** be used in solutions provided to Miami-Dade County.
- **Compensating Controls:** For any "N" responses, please provide detailed explanations of compensating controls or alternative solutions in the 'Detailed Explanation' column.
- **Evidence and Documentation:** Please provide supporting documents where applicable, such as SBOM files, policy documents, certificates, audit reports, or AI/ML governance frameworks.
- **Priority Levels:** Some functionalities may be marked as High Priority. These are critical requirements that must be met for compliance.
- **Data Protection Regulations:** Ensure compliance with relevant data protection laws such as GDPR, CCPA, or other applicable regulations.
- **Ethical AI Practices:** Adherence to ethical guidelines in AI development and deployment is crucial for maintaining trust and compliance.
- **SBOM Importance:** Maintaining an accurate and up-to-date SBOM is essential for supply chain security and vulnerability management.

Glossary of Terms and Acronyms

- **2FA:** Two-Factor Authentication
- **ADFS:** Active Directory Federation Services
- **AES:** Advanced Encryption Standard
- **AGPL:** GNU Affero General Public License
- **AI:** Artificial Intelligence
- **AI RMF:** Artificial Intelligence Risk Management Framework
- **API:** Application Programming Interface
- **CJIS:** Criminal Justice Information Services
- **CIS Controls:** Center for Internet Security Controls
- **CISO:** Chief Information Security Officer
- **CycloneDX:** A software bill of materials (SBOM) standard designed for use in application security contexts and supply chain component analysis
- **DDoS:** Distributed Denial of Service
- **DBA:** Database Administrator
- **DBMS:** Database Management System
- **EDR:** Endpoint Detection and Response
- **EOL:** End of Life
- **FedRAMP:** Federal Risk and Authorization Management Program
- **FIDO2:** Fast Identity Online 2, an authentication standard that enables phishing-resistant authentication methods
- **FIM:** Federated Identity Management
- **gMSA:** Group Managed Service Accounts
- **Group Managed Service Accounts (gMSA):** A feature in Microsoft Windows Server that provides automatic password management and simplified Service Principal Name (SPN) management for service accounts running on multiple servers. gMSAs allow services to share a common identity across multiple servers or instances, enhancing security and ease of management.
- **HIPAA:** Health Insurance Portability and Accountability Act
- **HR:** Human Resources
- **IDS/IPS:** Intrusion Detection System/Intrusion Prevention System
- **ISO/IEC 27001:** International Organization for Standardization/International Electrotechnical Commission 27001
- **MFA:** Multi-Factor Authentication
- **ML:** Machine Learning
- **NIST:** National Institute of Standards and Technology
- **NIST CSF:** NIST Cybersecurity Framework
- **OWASP:** Open Web Application Security Project
- **PCI DSS:** Payment Card Industry Data Security Standard.
- **PHI:** Protected Health Information
- **PII:** Personally Identifiable Information
- **Phishing Resistant Authentication:** Authentication methods designed to prevent phishing attacks by eliminating reliance on shared secrets (like passwords) that can be stolen or intercepted. This typically

involves using cryptographic authentication techniques, such as hardware security keys compliant with FIDO2/WebAuthn standards, certificate-based authentication, or biometric factors.

- **RBAC:** Role-Based Access Control
- **RDBMS:** Relational Database Management System
- **SAML:** Security Assertion Markup Language
- **SBOM:** Software Bill of Materials
- **SIEM:** Security Information and Event Management
- **SHA:** Secure Hash Algorithm SHA-256 or better is required.
- **SNMP:** Simple Network Management Protocol. SNMP v.3 or better is required.
- **SOC 2:** System and Organization Controls 2
- **SOX:** Sarbanes-Oxley Act
- **SPDX:** Software Package Data Exchange, an open standard for communicating software bill of material information
- **SSAE 16:** Statement on Standards for Attestation Engagements No. 16
- **SSO:** Single Sign-On
- **StateRAMP:** State Risk and Authorization Management Program
- **TLS:** Transport Layer Security

References

- **NIST SP 800-161:** *Supply Chain Risk Management Practices for Federal Information Systems and Organizations*
 - Provides guidance on identifying, assessing, and mitigating risks throughout the supply chain at all levels of the organization.
 - [Link to NIST SP 800-161](#)
 - **CIS Controls v8:** Center for Internet Security Critical Security Controls Version 8
 - Control 2.3: Addressing software inventory and control.
 - **ISO/IEC 27001 A.18.1.3:** Protection of records
 - Ensures records are protected from loss, destruction, falsification, and unauthorized access or release.
 - **NIST.AI.600-1.pdf:** NIST Artificial Intelligence Risk Management Framework (AI RMF 1.0)
 - Provides guidelines for managing risks associated with AI systems to promote trustworthy and responsible AI.
 - [Link to NIST AI RMF 1.0](#)
-

Submission Guidelines

- **Deadline for Submission:** [Insert Deadline]
 - **Preferred Format:** Please return the completed matrix in a **machine-readable format (e.g., Word or PDF)**.
 - **Contact for Queries:** [Insert Contact Name and Email]
 - **Confidentiality Assurance:** Your responses will be treated confidentially and used solely for the purpose of assessing the security controls for the proposed system.
-

Vendor Declaration

- I hereby attest that the information provided in this security matrix is accurate and complete to the best of my knowledge.
 - **Authorized Signature:**
 - **Name:**
 - **Title:**
 - **Date:**
-