CONFIDENTIALITY/NON-DISCLOSURE AGREEMENT

THIS CONFIDENTIALITY/NON-DISCLOSURE AGREEMENT ("Agreement") is effective as of the date last written below and is by and between the New Jersey Office of Homeland Security and Preparedness ("NJOHSP") with its principal address at 1200 Negron Drive, Hamilton New Jersey 08691; the Department of the Treasury – Division of Purchase and Property ("Division"), with its principal place of business at 33 West State Street, Trenton New Jersey 08625 (hereinafter collectively referred to as "State") and _____, with its principal place of business at _____, its employees, agents, contractors, and legal representatives (hereinafter referred to as the "Vendor").

WHEREAS, the Vendor intends to submit a Quote to the State in response to a Bid Solicitation advertised by the Division; and

WHEREAS, the Vendor is required to complete the State of New Jersey Security Due Diligence Third-Party Information Security Questionnaire and provide applicable supporting documents (collectively "Security Questionnaire") regarding its security and privacy controls and include it with its Quote submitted to the Division; and

WHEREAS, NJOHSP will review the Security Questionnaire to determine whether the Vendor's security and privacy controls meet the State of New Jersey's objectives as outlined and documented in the Statewide Information Security Manual and the corresponding requirements in the Bid Solicitation; and

WHEREAS, the State recognizes that the information contained in the Security Questionnaire may contain Confidential Information;

NOW THEREFORE, in consideration of the mutual promises and covenants contained herein, the Vendor and the State do hereby agree as follows:

1. Confidential Information which may be included on the Security Questionnaire means all information, including data, disclosed directly or indirectly, through any means of communication (including in oral, written or digital form) or observation, by or on behalf of the Vendor to or for the benefit of NJOHSP or the Division and all information or data derived there from, that relates to the Vendor's security and privacy controls as contained or referenced in the Security Questionnaire;

2. Confidential Information shall not include information that: (a) is or becomes a part of the public domain through no act or omission of the other party, except that if the information or data is personally identifying to a person or entity regardless of whether it has become part of the public domain through other means, the other party must maintain full efforts under the Contract to keep it confidential; (b) was in the other party's lawful possession prior to the disclosure and had not been obtained by the other party either directly or indirectly from the disclosing party; (c) is lawfully disclosed to the other party by a third party without restriction on the disclosure; or (d) is independently developed by the other party;

3. The Vendor acknowledges that the NJOHSP and the Division are public agencies subject to the New Jersey Open Public Records Act, N.J.S.A. 47:1A-1 et seq. ("OPRA"), and the common law Right to Know. OPRA is generally construed in favor of granting public access to documents maintained in the course of its official business;

4. In the event that the NJOHSP or the Division receives an appropriate request pursuant to OPRA and/or the common law Right to Know related to the Vendor's Security Questionnaire, NJOHSP and the Division agree not to disclose the Confidential Information contained on the Vendor's Security Questionnaire to a third party;

5. Notwithstanding the requirements of this Agreement, NJOHSP or the Division may release the Security Questionnaire if directed to do so by operation of law, pursuant to a lawfully issued subpoena, or pursuant to a ruling by a court or arbitrator of competent jurisdiction. NJOHSP or the Division shall notify the Vendor, at the address listed above, of such ruling or directive upon being made aware of same;
6. This Agreement shall be governed by the applicable laws, regulations and rules of evidence of the State of New Jersey without reference to conflict of laws principles and any legal action regarding this Agreement shall be filed in the appropriate Division of the New Jersey Superior Court;

7. This is the complete Agreement between the State and the Vendor with respect to the treatment of the Security Questionnaire and shall have no effect on the other components of the Vendor's submitted Quote; and

8. Any revision to this standard Agreement by the Vendor that was not approved and accepted by the State during the Question and Answer period shall render the Agreement VOID and the Agreement shall have no legal effect. Such revision, however, will not affect NJOHSP's review of the Security Questionnaire.

IN WITNESSETH WHEREOF, the State and Vendor have executed this Agreement, effective as of the date signed below by the Vendor.

FOR THE STATE OF NEW JERSEY

Michael T. Geraghty

Michael T. Geraghty
Chief Information Security Officer - State of New Jersey
Director – NJ Cybersecurity and Communications Integration Cell | NJCCIC
Office of Homeland Security and Preparedness

Amy F. Davis

Amy Davis, Acting Director
Department of the Treasury
Division of Purchase and Property

FOR THE VENDOR

Signature

Date

Print Name and Title

State of New Jersey
Security Due Diligence
Third-Party Information Security Questionnaire

Bid Solicitation #: 25DPP01119

Project: T2555 Internet-Based Patient Safety Adverse Event Reporting System

Date: _____

Published by:
New Jersey Cybersecurity and Communications Integration Cell

TABLE OF CONTENTS

INTRODUCTION ____ 4

INSTRUCTIONS ____ 4

CONFIDENTILIATY OF THIRD-PARTY INFORMATION SECURITY QUESTIONNAIRE SUBMISSIONS ____ 4

ABOUT THE NEW JERSEY CYBERSECURITY AND COMMUNICATIONS INTEGRATION CELL (NJCCIC) ____ 5

SECTION I – DATA SECURITY CATEGORIZATION ____ 6

- DESCRIPTION OF SERVICES ____ 6
- DATA SECURITY CATEGORIZATION ____ 6

SECTION II – DATA HOSTING AND SERVICES ____ 7

- DATA HOSTING AND SERVICES ____ 7

SECTION III – THIRD-PARTY ORGANIZATION ____ 8

- THIRD-PARTY ORGANIZATION PROFILE ____ 8
- SUBMITTER'S CONTACT INFORMATION ____ 8
- THIRD-PARTY INFORMATION SECURITY OFFICER CONTACT INFORMATION ____ 8

SECTION IV – THIRD-PARTY INFORMATION SECURITY QUESTIONNAIRE ____ 8

- 1.0 – INFORMATION SECURITY PROGRAM MANAGEMENT (PM) ____ 9
- 2.0 – COMPLIANCE (CP) ____ 10
- 3.0 – PERSONNEL SECURITY (PS) ____ 11
- 4.0 – SECURITY AWARENESS AND TRAINING (AW) ____ 12
- 5.0 – RISK MANAGEMENT (RM) ____ 13
- 6.0 – PRIVACY (PR) ____ 14
- 7.0 – ASSET MANAGEMENT (AM) ____ 14
- 8.0 – SECURITY CATEGORIZATION (SC) ____ 15
- 9.0 – MEDIA AND CRYPTOGRAPHY PROTECTION (MP) ____ 15
- 10.0 – ACCESS MANAGEMENT, IDENTITY, AND AUTHENTICATION (AC) ____ 16
- 11.0 – SECURITY ENGINEERING AND ARCHITECTURE (SE) ____ 17
- 12.0 – CONFIGURATION MANGAEMENT (CM) ____ 17
- 13.0 – ENDPOINT SECURITY (ES) ____ 18
- 14.0 – ISC/SCADA/OT SECURITY (OT) ____ 19
- 15.0 – INTERNET OF THINGS SECURITY (IT) ____ 20
- 16.0 – MOBILE DEVICE SECURITY (MD) ____ 20
- 17.0 – NETWORK SECURITY (NS) ____ 21

18.0 – CLOUD SECURITY (CL) 21
19.0 – CHANGE MANAGEMENT (CH) 22
20.0 – MAINTENANCE (MA) 22
21.0 – THREAT MANAGEMENT (TM) 23
22.0 – VULNERABILITY AND PATCH MANAGEMENT (VU) 23
23.0 – CONTINUOUS MONITORING (CO) 24
24.0 – SYSTEM DEVELOPMENT AND ACQUISITION (SD) 25
25.0 – PROJECT AND RESOURCE MANAGEMENT (PM) 27
26.0 – CAPACITY AND PERFORMANCE MANAGEMENT (CA) 27
27.0 – THIRD-PARTY MANAGEMENT (TP) 28
28.0 – PHYSICAL AND ENVIRONMENTAL SECURITY (PE) 28
29.0 – CONTINGENCY PLANNING (CT) 29
30.0 – INCIDENT RESPONSE (IR) 30
SECTION V – SUPPORTING DOCUMENTATION TO BE SUBMITTED 31
APPENDIX A – GLOSSARY 32

INTRODUCTION

The State of New Jersey's Third-Party Information Security Questionnaire is intended to ensure the security and privacy of State information systems and information, regardless of the location or the party responsible for providing the systems, applications, or services. The Questionnaire is aligned with the controls and security objectives as documented in the Statewide Information Security Manual (SISM) has which been derived from applicable State and federal laws; industry best practices including the National Institute of Standards and Technology (NIST) Cybersecurity Framework for Improving Critical Infrastructure; the Center for Internet Security (CIS) Top 20 Critical Security Controls; the Cloud Security Alliance (CSA) Cloud Controls Matrix (CCM); lessons learned; and other New Jersey State Government business and technology related considerations.

INSTRUCTIONS

All vendors, business partners, and other third-parties, collectively referred to as organizations in this document, are required to implement security and privacy controls that are commensurate with the criticality and sensitivity of the State of New Jersey information systems and information they develop, implement, provide, manage, host, or access. The Third-Party Information Security Questionnaire informs the State as to the degree to which the organization conforms to the State's information security requirements.

Organizations that:

a) Develop, implement, provide, manage, or host State of New Jersey major systems and applications;
b) Develop, implement, provide, manage, or host State of New Jersey general support systems; and/or
c) Have authorized access to State systems production environments, internal networks, and/or sensitive information

are required to complete and submit the Third-Party Information Security Questionnaire. By submitting a Third-Party Information Security Questionnaire to the NJCCIC, the submitting individual attests to its truth and accuracy to the best of their knowledge at the time the submission is made.

In some cases, the State may require additional clarifying information, documentation, and copies of certifications and attestations beyond what was initially provided by the submitting organization. A submission shall not be considered complete until the NJCCIC receives all necessary documentation and completes a Third-Party Information Security Risk Assessment Report.

Based on the overall risk rating as determined by the NJCCIC, the sponsoring Agency will determine if the risk rating is acceptable to proceed for the given engagement. Based on the criticality and/or sensitivity of the information system and information in scope, as well as the legal, regulatory, and/or contractual requirements, the State may require the submitting organization to implement additional risk mitigation controls prior to the award of any contract or agreement.

CONFIDENTIALITY OF THIRD-PARTY INFORMATION SECURITY QUESTIONNAIRE SUBMISSIONS

An uncompleted Third-Party Information Security Questionnaire is considered a public document. It may be disseminated via authorized channels and requires no confidentiality protections. A completed Third-Party Information Security Questionnaire along with all supporting documentation would inherently include administrative or technical information regarding computer hardware, software, and networks which, if disclosed would jeopardize computer security of the submitting organization and/or the State of New Jersey. As such, to the extent permitted by law, all non-public information submitted as part of a completed Third-Party Information Security Questionnaire, including but not limited to supporting documents, records, notes, written comments, reports, or analysis generated in or in the execution of a vendor's submission shall be treated and deemed as confidential and exempt from public disclosure under the State of New Jersey Open Public Records Act (N.J.S.A. 47:1A-1 et seq.) and the Domestic Security Preparedness Act P.L. 2001, c.246.

ABOUT THE NEW JERSEY CYBERSECURITY AND COMMUNICATIONS INTEGRATION CELL (NJCCIC)

The New Jersey Cybersecurity and Communications Integration Cell is a component organization within the New Jersey Office of Homeland Security and Preparedness (OHSP). The NJCCIC is comprised of OHSP, Office of Information Technology, and New Jersey State Police personnel working in concert to make New Jersey more resilient to cyber threats. As part of its portfolio of duties, the NJCCIC is responsible for conducting information security risk assessments of third parties with access to State of New Jersey information assets.

For more information about the NJCCIC, please visit www.cyber.nj.gov or contact us at njccic@cyber.nj.gov or 1.833.4-NJCCIC.

SECTION I – DATA SECURITY CATEGORIZATION

DESCRIPTION OF SERVICES

Provide a description of the project and services provided to the State of New Jersey or the purpose of the access to State information systems, internal networks, and/or sensitive information:

The Patient Safety Reporting System (PSRS) is a confidential electronic reporting system for licensed facilities in New Jersey required to report Patient Safety events based on the requirements in the Patient Safety Regulations under N.J.A.C. 8:43E-10. The RFP is for professional services to maintain the PSRS application, and providing the technical and programming support needed to ensure our compliance. All PSRS server infrastructure is currently hosted at New Jersey Office of Information Technology (NJOIT).

DATA SECURITY CATEGORIZATION

Select the data types that will be generated, accessed, processed, stored, and/or transmitted for this engagement with the State of New Jersey.

☐	**Public or Non-Sensitive Data**		
☑	**Sensitive Data**	**Personally Identifiable Information:**	☑
		Social Security Numbers:	☐
		Personal Health Information or ePHI:	☑
		Financial Information:	☐
		Tax Related Information:	☐
		Criminal Justice or Law Enforcement Information:	☐
		Critical Infrastructure Information:	☐
		Other Sensitive Information not listed above:	☑

List the specific data elements (i.e., first and last name, email address, IP address, etc.) involved as a part of this engagement with the State of New Jersey:

Business Sensitive Data, and other data elements including, but not limited to:

- First and last name, and date of birth of the patient and the facility users;
- Date of admission;
- Location and severity of injury; and
- Date, time, and location of the event.

SECTION II – DATA HOSTING AND SERVICES

DATA HOSTING AND SERVICES	
For the following questions, please provide accurate responses as they apply to the scope of the anticipated engagement with the State of New Jersey.	
1.	Is the product considered SaaS or cloud hosted? ☐ **Yes** ☐ **No**
2.	Which cloud hosting provider does this engagement leverage? ☐ **AWS** ☐ **Azure** ☐ **Google** ☐ **Private** ☐ **N/A**
3.	Please indicate the cloud environment provided for the State of NJ. ☐ **Commercial** ☐ **Government** ☐ **N/A** Is a Government cloud environment available for the State? ☐ **Yes** ☐ **No**
4.	Confirm all State of NJ data strictly resides within the United States in compliance with the State's information security expectations. ☐ **Yes** ☐ **No**
5.	Provide the general location of where data is stored (e.g., US-East, US-West, or the name of the State where servers are located).
6.	Is the product or service FedRAMP or StateRAMP authorized? ☐ **FedRAMP** ☐ **StateRAMP** ☐ **No** Please indicate the FedRAMP or StateRAMP impact level. ☐ **Low** ☐ **Moderate** ☐ **High**
7.	Please describe the screening and background checks you conduct for your workforce (personnel, contractors, and third parties) that have access to sensitive information.
8.	If State of NJ data is accessed, indicate the devices your workforce will use. ☐ **Personal** ☐ **Company owned** ☐ **State of NJ owned**
9.	Will State of NJ data be accessed or handled by any third party or subcontractor for the purposes of this engagement? ☐ **Yes** ☐ **No** If yes, please indicate the third party and the services provided.

SECTION III – THIRD-PARTY ORGANIZATION INFORMATION

THIRD-PARTY ORGANIZATION PROFILE	
Organization Name:	**State:**
Mailing Address:	**Zip/Postal Code:**
City:	**Country:** United States
Organization Website URL: https://	
SUBMITTER'S CONTACT INFORMATION	
First Name:	**Email Address:**
Last Name:	**Phone #:**
Title:	
THIRD-PARTY ORGANIZATION INFORMATION SECURITY OFFICER CONTACT INFORMATION	
First Name:	**Email Address:**
Last Name:	**Phone #:**
THIRD-PARTY INFORMATION SECURITY QUESTIONNAIRE	
Date Submitted:	

SECTION IV – THIRD-PARTY INFORMATION SECURITY QUESTIONNAIRE

For each of the control areas below, please provide accurate responses as they apply to your information security program and the scope of the anticipated engagement with the State of New Jersey. You are required to provide answers for all controls and questions as it applies to the scope of your engagement with the State of New Jersey. For any of the control areas or supplemental information questions in which you answer "No" or "N/A" (Not Applicable) please provide additional information explaining your answers in the "Optional - Please provide any additional information" text field. Some control areas include supplemental questions and may require additional documentation to be submitted.

1.0 – INFORMATION SECURITY PROGRAM MANAGEMENT (PM)	
1.1 – The organization establishes and maintains a framework to provide assurance that information security strategies are aligned with and support the State's business objectives, are consistent with applicable laws and regulations through adherence to policies and internal controls, and provide assignment of responsibility, all in an effort to manage risk. Information security program management includes, at a minimum, the following: • Establishment of a management structure with clear reporting paths and explicit responsibility for information security; • Creation, maintenance, and communication of information security policies, standards, procedures, and guidelines to include the control areas listed below; • Development and maintenance of relationships with external organizations to stay abreast of current and emerging security issues and for assistance, when applicable; and • Independent review of the effectiveness of the organization's information security program.	No
Supplemental Information	
1.2 – Do you align your information security program following industry standard frameworks such as the NIST CSF, ISO 27001, CIS Top 20, CoBIT? If yes, please list which framework(s) you employ.	
1.3 – Describe the process you follow, and how frequently, to review and update your security program and safeguards?	
1.4 – If you employ an Exception Management Policy please document the processes for the submission, review, documentation, and the application of exceptions to compliance with established information security policies and standards.	
1.5 – Please detail your disciplinary or sanction policy established for personnel and contractors who have violated security policies and procedures?	
1.6 – Optional - Please provide any additional information relative to this control area.	

2.0 – COMPLIANCE (CP)

2.1 – The organization develops, implements, and governs processes to ensure compliance with all applicable statutory, regulatory, contractual, and internal policy obligations. Ensuring compliance includes, at a minimum: No

- Statutory, Regulatory, and Contractual Compliance;
- Security controls oversight; and
- Periodically conducting security assessments.

Supplemental Information

2.2 – Indicate all third-party security audits, and subsequent last audit dates, conducted at your organization to ensure compliance with applicable laws, regulations and contractual requirements.

- ☐ CJIS
- ☐ IRS-1075
- ☐ FISMA
- ☐ SOC2
- ☐ PCI-DSS
- ☐ Social Security Admin.
- ☐ FedRAMP
- ☐ Other:

2.3 – Specify all compliance frameworks and standards your organization follows (e.g., GDPR, COBIT, ISO, etc.). Please provide documentation for all IT operational, security, and privacy-related standards, certifications, and/or regulations for which your organization or the intended product/system/application/service is compliant.

2.4 – Optional - Please provide any additional information relative to this control area.

3.0 – PERSONNEL SECURITY (PS)	
3.1 – The organization implements processes to ensure all personnel, with access to relevant State information, have the appropriate background, skills, and training to perform their job responsibilities in a competent, professional, and secure manner. Workforce security controls include, at a minimum: • Position descriptions that include appropriate language regarding each role's security requirements; • To the extent permitted by law, employment screening checks are conducted and successfully passed for all personnel prior to beginning work or being granted access to organization information assets; • Rules of behavior are established and procedures are implemented to ensure personnel are aware of and understand usage policies applicable to the organization's information and information systems; • Access reviews are conducted upon personnel transfers and promotions to ensure access levels are appropriate; • Disabling system access for terminated personnel and collecting all organization owned assets prior to the individual's departure; and • Procedures are implemented that ensure all personnel are aware of their duty to protect organizational information assets and their responsibility to immediately report any suspected information security incidents.	No
Supplemental Information	
3.2 – Please describe the screening and background checks you conduct for your workforce (personnel, contractors, and third-parties) that have access to sensitive information (e.g., CJI, FTI, PCI, etc.).	
3.3 – Are all personnel required to sign an Acceptable Use Policy (AUP)? If you answered yes, please submit a copy of the AUP. If no, please explain.	
3.4 – Describe the procedures the organization follows to govern changes in employment (transfers, promotions, etc.) and/or termination of staff.	
3.5 – Optional - Please provide any additional information relative to this control area.	

4.0 – SECURITY AWARENESS AND TRAINING (AW)	
4.1 – The organization provides periodic and on-going information security awareness and training to ensure personnel are aware of information security risks and threats, understand their responsibilities, and are aware of the statutory, regulatory, contractual, and policy requirements that are intended to protect information systems and State Confidential Information from a loss of confidentiality, integrity, availability and privacy. Security awareness and training includes, at a minimum: • Personnel are provided with security awareness training upon hire and at least annually, thereafter; • Security awareness training records are maintained as part of the personnel record; • Role-based security training is provided to personnel with respect to their duties or responsibilities (e.g. network and systems administrators require specific security training in accordance with their job functions); and • Individuals are provided with timely information regarding emerging threats, best practices, and new policies, laws, and regulations related to information security.	No
Supplemental Information	
4.2 – Describe the security awareness and training program you provide to personnel and contractors to ensure they are aware of information security risks and threats, understand their responsibilities, and are aware of the statutory and policy requirements. Is the training mandatory? How is training by personnel documented and tracked? How often is security awareness training conducted?	
4.3 – Optional - Please provide any additional information relative to this control area.	

5.0 – RISK MANAGEMENT (RM)	
5.1 – The organization establishes requirements for the identification, assessment, and treatment of information security risks to operations, information, and/or information systems. Risk management requirements shall include, at a minimum: • Categorizing systems and information based on their criticality and sensitivity; • Ensuring risks are identified, documented and assigned to appropriate personnel for assessment and treatment; • Ensuring risk assessments are conducted throughout the lifecycles of information systems to identify, quantify, and prioritize risks against operational and control objectives and to design, implement, and exercise controls that provide reasonable assurance that security objectives will be met; and • Mitigating risks to an acceptable level and prioritizing remediation actions based on risk criteria and establishing timelines for remediation. Risk treatment may also include the acceptance or transfer of risk.	No
Supplemental Information	
5.2 – Describe the risk management processes you employ that account for the identification, assessment, and treatment of risks that can adversely impact the confidentiality, integrity, and availability of the product/system/application/service. How often are these risk management processes performed?	
5.3 – Describe how risks and risk mitigation efforts are evaluated and prioritized. Include details on how you document and verify the results of these risk mitigation processes?	
5.4 – Optional - Please provide any additional information relative to this control area.	

6.0 – PRIVACY (PR)	
6.1 – The organization establishes appropriate processes and safeguards necessary to protect the personally identifiable information (PII) that the organization collects, stores, processes, uses, and transmits on behalf of the State of New Jersey. Privacy controls and processes include, but are not limited to: • Ensuring only the minimum amount of PII necessary to carry out the business function, and in accordance with applicable laws and regulations, is collected and stored; • Safeguarding PII through the implementation of administrative, physical, and technical controls (e.g., access controls, encryption and tokenization, etc.); and • Securely deleting PII when no longer necessary for business or legal purposes.	No
Supplemental Information	
6.2 – Describe your privacy program and detail how it maintains currency with evolving applicable privacy requirements. Please submit a copy of or provide a link to your privacy program.	
6.3 – Optional - Please provide any additional information relative to this control area.	

7.0 – ASSET MANAGEMENT (AM)	
7.1 – The organization implements administrative, technical, and physical controls necessary to safeguard information technology assets from threats to their confidentiality, integrity, or availability, whether internal or external, deliberate or accidental. Asset management controls include, but are not limited to: • Information technology asset identification and inventory; • Assigning custodianship of assets; and • Restricting the use of non-authorized devices.	No
Supplemental Information	
7.2 – Optional - Please provide any additional information relative to this control area.	

8.0 – SECURITY CATEGORIZATION (SC)

8.1 – The organization implements processes that classify information and categorize information systems throughout their lifecycles according to their sensitivity and criticality, along with the risks and impact should there be a loss of confidentiality, integrity, availability, or breach of privacy. Information classification and system categorization includes labeling and handling requirements. Security Categorization controls include, but are not limited to, the following:

No

- Implementing a data protection policy;
- Classifying data and information systems in accordance with their sensitivity and criticality;
- Masking sensitive data that is displayed or printed; and
- Implementing handling and labeling procedures.

Supplemental Information

8.2 – Optional - Please provide any additional information relative to this control area.

9.0 – MEDIA AND CRYPTOGRAPHIC PROTECTION (MP)

9.1 – The organization establishes controls to ensure data and information, in all forms and mediums, are protected throughout their lifecycles based on their sensitivity, value, and criticality, and the impact that a loss of confidentiality, integrity, availability, and privacy would have on the organization, business partners, or individuals. Media protections include, but are not limited to:

No

- Media storage/access/transportation;
- Maintenance of sensitive data inventories;
- Application of cryptographic protections;
- Restricting the use of portable storage devices;
- Establishing records retention requirements in accordance with business objectives and statutory and regulatory obligations; and
- Media disposal/sanitization.

Supplemental Information

9.2 – Detail the mechanisms used to secure data at rest, data in transit, and data in use.

9.3 – Describe cryptographic standards and technologies employed to protect sensitive State of New Jersey data. Include details on the encryption or hashing algorithms used, key management processes, use of hardware or software key storage, key fragmentation, etc.

9.4 – Optional - Please provide any additional information relative to this control area.

10.0 – ACCESS MANAGEMENT, IDENTITY, AND AUTHENTICATION (AC)	
10.1 – The organization establishes security requirements and ensures appropriate mechanisms are provided for the control, administration, and tracking of access to, and the use of, the organization's information systems. Access management includes, at a minimum: • Ensuring the principle of least privilege is applied for specific duties and information systems (including specific functions, ports, protocols, and services) so processes operate at privilege levels no higher than necessary to accomplish required organizational missions and/or functions; • Implementing account management processes for registration, updates, changes, and de-provisioning of system access; • Ensuring the principle of least privilege when provisioning access to organizational assets; • Provisioning access according to an individual's role and business requirements for such access; • Implementing the concept of segregation of duties by disseminating tasks and associated privileges for specific sensitive duties among multiple people; • Establishing and managing unique identifiers (e.g., User-IDs) and secure authenticators (e.g., passwords, biometrics, personal identification numbers, etc.) to support nonrepudiation of activities by users or processes; • Implementing multi-factor authentication (MFA) requirements for access to sensitive and critical systems, and for remote access to the organization's systems and information; and • Conducting periodic reviews of access authorizations and controls.	No
Supplemental Information	
10.2 – Describe your organization's processes and methods utilized for granting access, reviewing access, and documenting the review. Do you centrally manage access throughout the organization? Explain in detail.	
10.3 – Detail your password and authentication policy and standards. Include minimum length, lockout, complexity, timeout period, password history, etc. How are these managed and enforced?	
10.4 – Describe the process of controlling and monitoring the use of privileged and administrative accounts within your organization. Is Multi-Factor Authentication (MFA) required for privileged access? Do end-users have local administrator access?	
10.5 – If personnel and/or contractors are provided with remote access to your organization's internal network, please describe the mechanisms used for authentication and authorization. Detail the use of MFA for remote access, if applicable.	
10.6 – Optional - Please provide any additional information relative to this control area.	

11.0 – SECURITY ENGINEERING AND ARCHITECTURE (SE)

11.1 – The organization employs security engineering and architecture principles for all information technology assets, such that they incorporate industry recognized leading security practices and address applicable statutory and regulatory obligations. Applying security engineering and architecture principles include, at a minimum:

No

- Implementing configuration standards that are consistent with industry-accepted system hardening standards and addressing known security vulnerabilities for all system components;
- Establishing a defense in-depth security posture that includes layered technical, administrative, and physical controls;
- Incorporating security requirements into the systems throughout their life cycles;
- Delineating physical and logical security boundaries;
- Tailoring security controls to meet organizational and operational needs;
- Performing threat modeling to identify use cases, threat agents, attack vectors, and attack patterns as well as compensating controls and design patterns needed to mitigate risk;
- Implementing controls and procedures to ensure critical systems fail-secure and fail-safe in known states; and
- Ensuring information system clock synchronization across the organization.

Supplemental Information

11.2 – Optional - Please provide any additional information relative to this control area.

12.0 – CONFIGURATION MANAGEMENT (CM)

12.1 – The organization ensures that baseline configuration settings are established and maintained in order to protect the confidentiality, integrity, and availability of all information technology assets. Secure configuration management includes, but is not limited to:

No

- Hardening systems through baseline configurations; and
- Configuring systems in accordance with the principle of least privilege to ensure processes operate at privilege levels no higher than necessary to accomplish required functions.

Supplemental Information

12.2 – Describe the processes employed to establish and maintain baseline security configuration settings across your organization. Industry standard configuration and hardening standards include, but are not limited to, CIS Benchmarks, DISA STIGs, and component vendor security configuration guides.

12.3 – Describe the processes and protective technologies employed to verify these security configuration settings are maintained and to detect any attempts to adversely impact the confidentiality, integrity, and availability of components or data in your organization. Protective technologies include, but are not limited to, firewalls, host and network intrusion detection/protection systems, file integrity monitoring, and anti-malware software.
12.4 – Optional - Please provide any additional information relative to this control area.

13.0 – ENDPOINT SECURITY (ES)	
13.1 – The organization ensures that endpoint devices are properly configured, and measures are implemented to protect the organization's information and information systems from a loss of confidentiality, integrity, and availability. Endpoint security includes, at a minimum: • Maintaining an accurate and updated inventory of endpoint devices; • Applying security categorizations and implementing commensurate safeguards on endpoints; • Maintaining currency with operating system and software updates and patches; • Establishing physical and logical access controls; • Applying data protection measures (e.g., cryptographic protections); • Implementing anti-malware software, host-based firewalls, and port and device controls; • Implementing host intrusion detection and prevention systems (HIDS/HIPS) where applicable; • Restricting access and/or use of ports and I/O devices; and • Ensuring audit logging is implemented and logs are reviewed on a continuous basis.	No
Supplemental Information	
13.2 – Describe the standard personnel issued device security configuration/features (Login Password, anti-malware, Full Disk Encryption, Administrative Privileges, Firewall, Auto-lock, etc.).	
13.3 – Are all endpoints in or with access to the production environment centrally managed? Explain.	

13.4 – Describe how you limit data exfiltration of sensitive data from endpoints in or with access to the production environment.
13.5 – Optional - Please provide any additional information relative to this control area.

14.0 – ICS/SCADA/OT SECURITY (OT)	
14.1 – The organization implements controls and processes to ensure risks, including risks to human safety, are accounted for and managed in the use of Industrial Control Systems (ICS), Supervisory Control and Data Acquisition (SCADA) systems, and Operational Technologies (OT). ICS/SCADA/OT Security requires the application of all of the enumerated control areas included here in this document, including, at a minimum: • Conducting risk assessments prior to implementation and throughout the lifecycles of ICS/SCADA/OT assets; • Developing policies and standards specific to ICS/SCADA/OT assets; • Ensuring the secure configuration of ICS/SCADA/OT assets; • Segmenting ICS/SCADA/OT networks from the rest of the organization's networks; • Ensuring least privilege and strong authentication controls are implemented; • Implementing redundant designs or failover capabilities to prevent business disruption or physical damage; and • Conducting regular maintenance on ICS/SCADA/OT systems.	No
Supplemental Information	
14.2 – As applicable, list and describe any ICS/SCADA/OT systems used across your organization and detail how those systems are secured physically, administratively, and technically.	
14.3 – Optional - Please provide any additional information relative to this control area.	

15.0 – INTERNET OF THINGS SECURITY (IT)	
15.1 – The organization implements controls and processes to ensure risks are accounted for and managed in the use of Internet of Things (IoT) devices including, but not limited to, physical devices, vehicles, appliances and other items embedded with electronics, software, sensors, actuators, and network connectivity which enables these devices to connect and exchange data. IoT security includes, at a minimum: • Developing policies and standards specific to IoT assets; • Ensuring the secure configuration of IoT assets; • Conducting risk assessments prior to implementation, and throughout the lifecycles of IoT assets; • Segmenting IoT networks from the rest of the organization's networks; and • Ensuring least privilege and strong authentication controls are implemented.	No
Supplemental Information	
15.2 – As applicable, list and describe any IoT devices used across your organization and detail how those devices are secured physically, administratively, and technically. Include information on network segmentation, access and authentication, and security updates.	
15.3 – Optional - Please provide any additional information relative to this control area.	

16.0 – MOBILE DEVICE SECURITY (MD)	
16.1 – The organization establishes administrative, technical, and physical security controls required to effectively manage the risks introduced by mobile devices used for organizational business purposes. Mobile device security includes, at a minimum: • Establishing requirements for authorization to use mobile devices for organizational business purposes; • Establishing Bring Your Own Device (BYOD) processes and restrictions; • Establishing physical and logical access controls; • Implementing network access restrictions for mobile devices; • Implementing mobile device management solutions to provide centralized management of mobile devices and to ensure technical security controls (e.g., encryption, authentication, remote-wipe, etc.) are implemented and updated as necessary; • Establishing approved application stores from which applications can be acquired; • Establishing lists of approved applications that can be used; and • Training of mobile device users regarding security and safety.	No

Supplemental Information
16.2 – Does your organization allow for BYOD devices to connect to your internal network? If so, how are BYOD managed so they do not introduce additional risks?
16.3 – Optional - Please provide any additional information relative to this control area.

17.0 – NETWORK SECURITY (NS)	
17.1 – The organization implements defense-in-depth and least privilege strategies for securing the information technology networks that they operate. To ensure information technology resources are available to authorized network clients and protected from unauthorized access, organizations must: • Include protection mechanisms for network communications and infrastructure (e.g., layered defenses, denial of service protection, encryption for data in transit, etc.); • Include protection mechanisms for network boundaries (e.g., limit network access points, implement firewalls, use Internet proxies, restrict split tunneling, etc.); • Control the flow of information (e.g., deny traffic by default/allow by exception, implement Access Control Lists, etc.); and • Control access to the organization's information systems (e.g., network segmentation, network intrusion detection and prevention systems, wireless restrictions, etc.).	No
Supplemental Information	
17.2 – Optional - Please provide any additional information relative to this control area.	

18.0 – CLOUD SECURITY (CL)	
18.1 – The organization establishes security requirements that govern the use of private, public, and hybrid cloud environments to ensure risks associated with a potential loss of confidentiality, integrity, availability, and privacy are managed. This includes, at a minimum: • Security is accounted for in the acquisition and development of cloud services; • The design, configuration, and implementation of cloud-based applications, infrastructure and system interfaces are conducted in accordance with mutually agreed-upon service, security, and capacity-level expectations; • Security roles and responsibilities for the organization and the cloud provider are delineated and documented; and • Controls necessary to protect sensitive data in public cloud environments are implemented.	No
Supplemental Information	
18.2 – Optional - Please provide any additional information relative to this control area.	

19.0 – CHANGE MANAGEMENT (CH)	
19.1 – The organization establishes controls required to ensure change is managed effectively. Organizations must ensure changes are appropriately tested, validated, and documented before implementing any change on a production network. Change management provides the organization with the ability to handle changes in a controlled, predictable, and repeatable manner, and to identify, assess, and minimize the risks to operations and security. Change management controls include, at a minimum: • Notifying all stakeholders of changes; • Conducting a security impact analysis for changes; and • Verifying security functionality after the changes have been made.	No
Supplemental Information	
19.2 – Describe the change control process as it relates to patches, hot-fixes, upgrades, and configuration changes within your organization. Include information on review of proposed changes. Include information on timelines used for testing, implementation, and emergency change control.	
19.3 – Optional - Please provide any additional information relative to this control area.	

20.0 – MAINTENANCE (MA)	
20.1 – The organization implements processes and controls to ensure that information assets are properly maintained, thereby minimizing the risks from emerging information security threats and/or the potential loss of confidentiality, integrity, or availability due to system failures. Maintenance security includes, at a minimum: • Conducting scheduled and timely maintenance; • Ensuring individuals conducting maintenance operations are qualified and trustworthy; and • Vetting, escorting, and monitoring third-parties conducting maintenance operations on the organization's information technology assets.	No
Supplemental Information	
20.2 – Optional - Please provide any additional information relative to this control area.	

21.0 – THREAT MANAGEMENT (TM)

21.1 – The organization establishes effective communication protocols and processes to collect and disseminate actionable threat intelligence, thereby providing component units and individuals with the information necessary to effectively manage risk associated with new and emerging threats to the organization's information technology assets and operations. Threat management includes, at a minimum:

No

- Developing, implementing, and governing processes and documentation to facilitate the implementation of a threat awareness policy, as well as associated standards, controls and procedures; and
- Subscribing to and receiving relevant threat intelligence information from the US CERT, the organization's vendors, and other sources as appropriate.

Supplemental Information

21.2 – List and describe the threat intelligence sources you subscribe to or follow in order to keep abreast of potential security vulnerabilities and threats.

21.3 – Optional - Please provide any additional information relative to this control area.

22.0 – VULNERABILITY AND PATCH MANAGEMENT (VU)

22.1 – The organization implements proactive vulnerability identification, remediation, and patch management practices to minimize the risk of a loss of confidentiality, integrity, and availability of information system, networks, components, and applications. Vulnerability and patch management practices include, at a minimum:

No

- Prioritizing vulnerability scanning and remediation activities based on the criticality and security categorization of the organization's systems and information, and the risks associated with a loss of confidentiality, integrity, availability, and/or privacy;
- Maintaining software and operating systems at the latest vendor-supported patch levels;
- Conducting penetration testing and red team exercises; and
- Employing qualified third-parties to conduct Independent vulnerability scanning, penetration testing, and red-team exercises.

Supplemental Information
22.2 – Describe your network vulnerability scanning and penetration testing process. Who conducts your network penetration testing and vulnerability scans? Are these vulnerability scans and penetration tests both external and internal? How often are vulnerability scans and penetration tests conducted?
22.3 – Describe how patches and vulnerability remediation processes prioritized. How do you document and verify the results of these remediation efforts?
22.4 – As applicable, please provide details on the most recent Application Code Review or Penetration Testing Reports carried out by independent third parties.
22.5 – Optional - Please provide any additional information relative to this control area.

23.0 – CONTINUOUS MONITORING (CO)	
23.1 – The organization implements continuous monitoring practices to establish and maintain situational awareness regarding potential threats to the confidentiality, integrity, availability, privacy, and safety of the organization's information and information systems through timely collection and review of security-related event logs. Continuous monitoring practices include, at a minimum: • Centralizing the collection and monitoring of event logs; • Ensuring the content of audit records includes all relevant security event information; • Protection of audit records from tampering; and • Detecting, investigating, and responding to incidents discovered through monitoring.	No
Supplemental Information	
23.2 – Describe the processes and technologies used for monitoring, alerting on, and logging of application, system, network, and security events. Include information on retention of logs and how they are reviewed.	
23.3 – Optional - Please provide any additional information relative to this control area.	

24.0 – SYSTEM DEVELOPMENT AND ACQUISITION (SD)	
24.1 – The organization establishes security requirements necessary to ensure that systems and application software programs developed by the organization or third-parties (e.g., vendors, contractors, etc.) perform as intended to maintain information confidentiality, integrity, and availability, and the privacy and safety of individuals. System development and acquisition security practices include, at a minimum: • Secure coding; • Separation of development, testing and operational environments; • Information input restrictions; • Input data validation; • Error handling; • Security testing throughout development; • Restrictions for access to program source code; and • Security training of software developers and system implementers.	No
Supplemental Information	
24.2 – As applicable, describe your Software Development Lifecycle (SDLC) including developers' access to production data, systems, and applications; version control tools used; promotion from development to production, etc.	
24.3 – As applicable, describe the processes you use to ensure code is being developed securely. Include details of the types of code reviews and analysis (e.g., static and dynamic) performed and how threat modeling is incorporated into the design phase of development.	
24.4 – As applicable, describe how you monitor for vulnerabilities in dependencies and third-party libraries or code included in the product/system/application/service.	
24.5 – Describe how API security is maintained including storage of API keys and support for IP whitelisting for API access.	

24.6 – As applicable, for web applications that require authentication as part of the product/system/application/service you're providing, please describe how you authenticate users. If passwords are used, describe complexity requirements, and how passwords are protected. If SAML, SSO and/or MFA is supported, please describe the available options.
24.7 – As applicable, describe additional user authentication controls including, but not limited to, IP whitelisting and geofencing.
24.8 – As applicable, describe the protective technologies (Web Application Firewalls, Proxies, etc.) that you employ to mitigate web application security risks (e.g., SQLi, XSS, XSRF, etc.).
24.9 – As applicable, describe the training you provide to developers with respect to secure coding practices and system development life cycle.
24.10 – Optional - Please provide any additional information relative to this control area.

25.0 – PROJECT AND RESOURCE MANAGEMENT (PM)	
25.1 – The organization ensures that controls necessary to appropriately manage risks are accounted for and implemented throughout the System Development Life Cycle (SDLC). Project and resource management security practices include, at a minimum: • Defining and implementing security requirements; • Allocating resources required to protect systems and information; and • Ensuring security requirements are accounted for throughout the SDLC.	No
Supplemental Information	
25.2 – Optional - Please provide any additional information relative to this control area.	

26.0 – CAPACITY AND PERFORMANCE MANAGEMENT (CA)	
26.1 – The organization implements processes and controls necessary to protect against avoidable impacts to operations by proactively managing the capacity and performance of its critical technologies and supporting infrastructure. Capacity and performance management practices include, but are not limited to, at a minimum: • Ensuring the availability, quality, and adequate capacity of compute, storage, memory, and network resources are planned, prepared, and measured to deliver the required system performance and future capacity requirements; and • Implementing resource priority controls to prevent or limit Denial of Service (DoS) effectiveness.	No
Supplemental Information	
26.2 – As applicable, describe the processes and controls that are employed to ensure information systems scale appropriately and meet availability needs. Include information on DDoS protections, automated provisioning of resources, high-availability, etc.	
26.3 – Optional - Please provide any additional information relative to this control area.	

27.0 – THIRD-PARTY MANAGEMENT (TP)

27.1 – The organization implements processes and controls to ensure that risks associated with third-parties (e.g., vendors, contractors, business partners, etc.) providing information technology equipment, software, and/or services are minimized or avoided. Third-Party management processes and controls include, at a minimum:

- Tailored acquisition strategies, contracting tools, and procurement methods for the purchase of systems, system components, or system service from suppliers;
- Due diligence security reviews of suppliers and third parties with access to the organization's systems and sensitive information;
- Third-Party interconnection security; and
- Independent testing and security assessments of supplier technologies and supplier organizations.

No

Supplemental Information

27.2 – Describe the processes utilized to validate third-party service providers' compliance with applicable laws, regulations, and contractual requirements.

27.3 – Optional - Please provide any additional information relative to this control area.

28.0 – PHYSICAL AND ENVIRONMENTAL SECURITY (PE)

28.1 – The organization establishes physical and environmental protection procedures that limit access to systems, equipment, and the respective operating environments, to only authorized individuals. The organization ensures appropriate environmental controls in facilities containing information systems and assets, to ensure sufficient environmental conditions exist to avoid preventable hardware failures and service interruptions. Physical and environmental controls include, at a minimum:

- Physical access controls (e.g., locks, security gates and guards, etc.);
- Visitor controls;
- Security monitoring and auditing of physical access;
- Emergency shutoff;
- Emergency power;
- Emergency lighting;
- Fire protection;
- Temperature and humidity controls;
- Water damage protection; and
- Delivery and removal of information assets controls.

No

Supplemental Information

28.2 – Optional - Please provide any additional information relative to this control area.

29.0 – CONTINGENCY PLANNING (CT)	
29.1 – The organization develops, implements, tests, and maintains contingency plans to ensure continuity of operations for all information systems that deliver or support essential or critical business functions on behalf of the organization. Contingency planning includes, at a minimum: • Backup and recovery strategies; • Continuity of operations; • Disaster recovery; and • Crisis management.	No
Supplemental Information	
29.2 – Describe the processes and plans that are implemented to ensure continuity of operations for your organization.	
29.3 – Describe the data and system backup/recovery processes employed and how the security categorization of the information is maintained in backup media. How often are backups tested to verify media reliability and information integrity? What are the recovery point and recovery time objectives?	
29.4 – As applicable, if an alternate site(s) has been established for storage, processing, and communications functions as part of the organization's contingency plan, describe the processes and timelines for failing over. Is the alternate site considered Hot, Warm, or Cold? Explain how often fail-over processes are tested and how results are documented and reviewed.	
29.5 – Optional - Please provide any additional information relative to this control area.	

30.0 – INCIDENT RESPONSE (IR)	
30.1 – The organization maintains an information security incident response capability that includes adequate preparation, detection, analysis, containment, recovery, and reporting activities. Information security incident response activities include, at a minimum: • Information security incident reporting awareness; • Incident response planning and handling; • Establishment of an incident response team; • Cybersecurity insurance; • Contracts with external incident response services specialists; and • Contacts with law enforcement cybersecurity units.	No
Supplemental Information	
30.2 – Describe how your incident response plan is tested and how often tests are conducted.	
30.3 – Describe in detail any breaches of information security your organization experienced over the past five years. Describe how affected customers were notified by your organization, the timeframe of such notifications, and steps taken by your organization to prevent the breach from recurring.	
30.4 – If the organization has purchased cybersecurity liability insurance describe in detail the scope of the coverage.	
30.5 – Optional - Please provide any additional information relative to this control area.	

SECTION V – SUPPORTING DOCUMENTATION TO BE SUBMITTED

Please submit the following supporting documentation with this questionnaire:

- The organization's Security Plan or written information security policies and standards ☐
- Privacy Policy ☐
- The organization's SOC2 Type II audit report ☐
- FedRAMP or StateRAMP Authorization ☐
- Independent information security audits and/or certifications (e.g., PCI-DSS, ISO27001, FISMA certification) ☐
- If the service/application you are proposing relies on subcontractors that handle State data, including Cloud Service Providers (CSP) (e.g., Amazon, Salesforce, Microsoft, Google, etc.), please submit relevant security profiles/certifications for the subcontractors, including CSPs, being utilized ☐
- Other relevant documentation, reports, information (please provide an explanation, as applicable)

APPENDIX A – GLOSSARY

Access: Ability and means to communicate with or otherwise interact with a system, to use system resources to handle information, to gain knowledge of the information the system contains, or to control system components and functions.

Access Control: The process of granting or denying specific requests to obtain and use information and related information processing services; and enter specific physical facilities.

Access Management: A discipline that focuses on ensuring that only approved roles are able to create, read, update, or delete data through appropriate and controlled methods.

Administrative Safeguards: Administrative actions, policies, and procedures to manage the selection, development, implementation, and maintenance of security measures to protect electronic health information and to manage the conduct of the covered entity's workforce in relation to protecting that information.

Alert: Notification that a specific attack has been directed at an organization's information systems.

Alternate Processing Site: Locations and infrastructures from which emergency or backup processes are executed, when the main premises are unavailable or destroyed.

Attack: An attempt to gain unauthorized access to system services, resources, or information, or an attempt to compromise system integrity.

Audit: Independent review and examination of records and activities to assess the adequacy of system controls, to ensure compliance with established policies and operational procedures, and to recommend necessary changes in controls, policies, or procedures.

Audit Log: A chronological record of system activities. Includes records of system access and operations performed in a given period.

Authenticate: To verify the identity of a user, user device, or other entity.

Authentication: The process of verifying the identity, or other attributes claimed by or assumed, of an entity (user, process, or device), or to verify the source and integrity of data.

Authorization: Access privileges granted to a user, program, or process, or the act of granting those privileges.

Availability: The property of being accessible and useable, upon demand, by an authorized entity.

Baseline Configuration: A set of specifications for a system, or Configuration Item (CI) within a system, that has been formally reviewed and agreed upon at a given point in time, which can be changed only through change control procedures. The baseline configuration is used as a basis for future builds, releases, and/or changes.

Best Practice: A proven activity or process that has been successfully used by multiple enterprises.

Boundary Protection: Monitoring and control of communications at the external boundary of an information system to prevent and detect malicious and other unauthorized communication, through the use of boundary protection devices (e.g., proxies, gateways, routers, firewalls, guards, encrypted tunnels).

Boundary Protection Device: A device with appropriate mechanisms that:

(i) Facilitates the adjudication of different interconnected system security policies (e.g., controlling the flow of information into or out of an interconnected system); and/or
(ii) Provides information system boundary protection.

Bring Your Own Device (BYOD): Refers to the policy of permitting personnel and contractors to use personally owned or third-party owned mobile devices for organizational business purposes.

Business Continuity Plan (BCP): The documentation of a predetermined set of instructions or procedures that describe how an organization's mission/business processes will be sustained during and after a significant disruption.

Cardholder Data: At a minimum, cardholder data consists of the full PAN. Cardholder data may also appear in the form of the full PAN plus any of the following: cardholder name, expiration date, and/or service code. See **Sensitive Authentication Data** for additional data elements that may be transmitted or processed (but not stored) as part of a payment transaction.

Change Control: A formal process used to ensure that a process, product, service, or technology component is modified only in accordance with agreed-upon rules. Many organizations have formal Change Control Boards that review and approve proposed modifications to technology infrastructures, systems, and applications. Data Governance programs often strive to extend the scope of change control to include additions, modifications, or deletions to data models and values for reference/master data.

Clear Text: Information that is not encrypted.

Cloud Computing: A model for enabling on-demand network access to a shared pool of configurable IT capabilities/resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. It allows users to access technology-based services from the network cloud without knowledge of, expertise with, or control over the technology infrastructure that supports them. This cloud model is composed of five essential characteristics (on-demand self-service, ubiquitous network access, location independent resource pooling, rapid elasticity, and measured service); three service delivery models (Cloud Software as a Service [SaaS], Cloud Platform as a Service [PaaS], and Cloud Infrastructure as a Service [IaaS]); and four models for enterprise access (Private cloud, Community cloud, Public cloud, and Hybrid cloud).

Cloud Service Provider: An entity that offers cloud-based platform, infrastructure, application, or storage services. Cloud service providers include internal entities, and external entities, such as Amazon, Microsoft, Salesforce, Google, and others.

Compensating Security Control: A management, operational, and/or technical control (i.e., safeguard or countermeasure) employed by an organization in lieu of a recommended security control in the low, moderate, or high baselines that provides equivalent or comparable protection for an information system.

Compromise: Disclosure of information to unauthorized persons, or a violation of the security policy of a system in which unauthorized intentional or unintentional disclosure, modification, destruction, or loss of an object may have occurred.

Confidentiality: The property that sensitive information is not disclosed to unauthorized individuals, entities, or processes.

Configuration Management: A structured process of managing and controlling changes to hardware, software, firmware, communications, and documentation throughout the system development life cycle.

Contingency Plan: Management policy and procedures used to guide an enterprise response to a perceived loss of mission capability. The Contingency Plan is the first plan used by the enterprise risk managers to determine what happened, why, and what to do. It may point to the Continuity of Operations Plan (COOP) or Disaster Recovery Plan for major disruptions.

Continuous Monitoring: The process implemented to maintain a current security status for individual information systems, or for the entire suite of information systems, on which the operational mission of the enterprise depends.

Control: A means of managing a risk or ensuring that an objective is achieved. Controls can be preventative, detective, or corrective and can be fully automated, procedural, or technology-assisted human-initiated activates. They can include actions, devices, procedures, techniques, or other measures.

Criminal Justice Information (CJI): The term used to refer to all FBI Criminal Justice Information Services (CJIS) provided data necessary for law enforcement and civil agencies to perform their missions including, but not limited to, data consisting of biometric, identity history, biographic, property, and case/incident history. The following categories of CJI describe the various data sets housed by the FBI CJIS architecture:

(i) Biometric Data – Data derived from one or more intrinsic physical or behavioral traits of humans typically for the purpose of uniquely identifying individuals from within a population. Biometric information used to identify individuals include fingerprints, palm prints, iris scans, and facial recognition data.

(ii) Identity History Data – Textual data that corresponds with an individual's biometric data, providing a history of criminal and/or civil events for the identified individual.

(iii) Biographic Data – Information about individuals associated with a unique case, and not necessarily connected to identity data. Biographic data does not provide a history of an individual, only information related to a unique case.

(iv) Property Data – Information about vehicles and property associated with crime when accompanied by any personally identifiable information (PII).

(v) Case/Incident History – Information about the history of criminal incidents.

Criticality: A measure of the degree to which an organization depends on the information or information system for the success of a mission or of a business function.

Cryptographic Key: A value used to control cryptographic operations, such as decryption, encryption, signature generation, or signature verification.

Cryptography: The discipline that embodies the principles, means, and methods for the transformation of data in order to hide their semantic content, prevent their unauthorized use, or prevent their undetected modification.

Data: A subset of information in an electronic format that allows it to be retrieved or transmitted.

Data Privacy: The assurance that a person's or organization's personal and private information is not inappropriately disclosed. Ensuring Data Privacy requires Access Management, eSecurity, and other data protection efforts. (SOURCE: Data Governance Institute)

Data Security: Protection of data from unauthorized (accidental or intentional) modification, destruction, or disclosure.

Defense-in-Depth: Information security strategy integrating people, technology, and operation capabilities to establish variable barriers across multiple layers and dimensions of the organization.

Denial of Service (DoS): The prevention of authorized access to resources or the delaying of time-critical operations. Depending on the service provided, time-critical may be defined at milliseconds or hours.

Disaster Recovery Plan (DRP): A written plan for recovering one or more information systems at an alternate facility in response to a major hardware or software failure or destruction of facilities.

Distributed Denial of Service (DDoS): A Denial of Service technique that uses numerous hosts to perform the attack.

Electronic Protected Health Information (ePHI): Electronic Protected Health Information (PHI) consists of any information about health status, provision of health care, or payment for health care that can be linked to an individual. PHI refers to all "individually identifiable information" held or transmitted by State entities or its business associates in any form or media, whether paper, electronic or oral. "Individually identifiable health information" is information, including demographic data, that relates to:

(i) The individual's past, present, or future physical or mental health or condition;

(ii) The provision of health care to the individual;

(iii) The past, present, or future payment for the provision of health care to the individual; or

(iv) The individual's identity for which there is a reasonable basis to believe it can be used to identify the individual.

Embedded System: An embedded system is a computer system with a dedicated function within a larger mechanical or electrical system, often with real-time computing constraints. It is embedded as part of a complete device often including hardware and mechanical parts.

Embedded Technology: Specialized hardware and software that is wholly incorporated as part of a larger system or machine.

Encryption: The process of changing plaintext into ciphertext for the purpose of security or privacy.

Endpoint: Any device capable of being connected, either physically or wirelessly to a network, and accepts communications back and forth across the network. Endpoints include, but are not limited to, computers, servers, tablets, mobile devices, or any similar network enabled device.

Entity: Either a subject (an active element that operates on information or the system state) or an object (a passive element that contains or receives information).

Federal Tax Information (FTI): FTI consists of federal tax returns (and information derived from it) that is in the agency's possession or control, which is covered by the confidentiality protections of the Internal Revenue Code (IRC) and subject to the IRC 6103(p)(4) safeguarding requirements including IRS oversight, including:

(i) Return information received directly from the IRS or obtained through an authorized secondary source, such as Social Security Administration (SSA), Federal Office of Child Support Enforcement (OCSE), Bureau of the Fiscal Service (BFS), Centers for Medicare and Medicaid Services (CMS), or another entity acting on behalf of the IRS pursuant to the IRC 6103(p)(2)(B) Agreement; and

(ii) Any information created by the recipient that is derived from federal return information received from the IRS or obtained through a secondary source.

Firewall: A gateway that limits access between networks in accordance with local security policy.

General Support System: An interconnected set of information resources under the same direct management control that shares common functionality. A general support system normally includes hardware, software, information, data, applications, communications, facilities, and people, which provides support for a variety of users and/or applications. A general support system, for example, can be a:

(i) Local Area Network (including workstations, printers, and other assets that support an agency office or facility);
(ii) Backbone Network (e.g., Department/Agency-wide and/or statewide (GSN));
(iii) Department/Agency information processing center, including its operating system and utilities (e.g., server room); and/or
(iv) Shared information processing service facility (e.g., State, or other, colocation data center).

Governance: Ensures that stakeholder needs, conditions, and options are evaluated to determine balanced, agreed upon enterprise objectives; setting direction through prioritization and decision making; and monitoring performance and compliance with direction and objectives.

Identification: The process of verifying the identity of a user, process, or device, usually as a prerequisite for granting access to resources in an IT system.

Industrial Control System: An information system used to control industrial processes such as manufacturing, product handling, production, and distribution. Industrial control systems include supervisory control and data acquisition systems (SCADA) used to control geographically dispersed assets, as well as distributed control systems (DCS) and smaller control systems using programmable logic controllers to control localized processes.

Information: Any communication or representation of knowledge such as facts, data, or opinions in any medium or form, including textual, numerical, graphic, cartographic, narrative, or audiovisual.

Information Asset: Any data, device, or other component of an information or communication system. Assets generally include hardware (e.g., servers, laptop and desktop computers, switches), software (e.g., commercial off the shelf and custom developed applications and support systems) and information. Assets may also be referred to as information resources or systems.

Information Security: The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide the confidentiality, integrity, and availability of information.

Information Security Classification: A system of designating security categories for information based on the impact to the business mission from loss of information confidentiality, integrity or availability (also classification, information classification, security classification)

Information System: A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.

Note: Information systems also include specialized systems such as industrial/process controls systems, telephone switching and private branch exchange (PBX) systems, and environmental control systems.

Information Technology: The term information technology includes computers, ancillary equipment, software, firmware, and similar procedures, services (including support services), and related resources.

Integrity: The property that sensitive data has not been modified or deleted in an unauthorized and undetected manner.

Internet: The single, interconnected, worldwide system of commercial, governmental, educational, and other computer networks that share:

(i) The protocol suite specified by the Internet Architecture Board (IAB); and

(ii) The name and address spaces managed by the Internet Corporation for Assigned Names and Numbers (ICANN).

Internet of Things (IoT): The network of physical devices, vehicles, home appliances, and other items embedded with electronics, software, sensors, actuators, and network connectivity, which enables these objects to connect and exchange data.

Intrusion Detection Systems (IDS): Hardware or software product(s) that gathers and analyzes information from various areas within a computer or a network to identify possible security breaches, which include both intrusions (attacks from outside the organizations) and misuse (attacks from within the organizations).

Intrusion Prevention Systems (IPS): Hardware or software product(s) that monitors network and/or system activities for malicious activity. The main functions of intrusion prevention systems are to identify malicious activity, log information about this activity, attempt to block/stop it, and report it.

IT Governance: The leadership, organizational structures, and processes that ensure that the enterprise's IT sustains and extends the enterprise's strategies and objectives.

Key: A value used to control cryptographic operations, such as decryption, encryption, signature generation, or signature verification.

Least Functionality: The principle of least functionality states that only the minimum access necessary to perform an operation should be granted to a user, a process, or a program, and that access should be granted only for the minimum amount of time necessary.

Least Privilege: The principle that a security architecture should be designed so that each entity is granted the minimum system resources and authorizations that the entity needs to perform its function.

Major Applications and Systems: Any system or application that includes one or more of the following characteristics:

(i) Users in more than one State Department/Agency;

(ii) Costs exceeds $250,000 to develop and implement (including the cost of hardware, software, and contract personnel);

(iii) Any public facing web application; and/or

(iv) Any application that stores or processes sensitive information or is deemed critical to the operations of the agency.

Malicious Code: Software or firmware intended to perform an unauthorized process that will have an adverse impact on the confidentiality, integrity, or availability of information system(s). A virus, worm, Trojan horse, or other code-based entity that infects a host. Spyware and some forms of adware are also examples of malicious code.

Malware: A program that is inserted into a system, usually covertly, with the intent of compromising the confidentiality, integrity, or availability of the victim's data, applications, or operating system or to otherwise annoy or cause disruption to the victim.

Media Sanitization: A general term referring to the actions taken to render data, written on media, unrecoverable by both ordinary and extraordinary means.

Minor Application: An application, other than a major application, that requires attention to security due to the risk and magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of the information in the application. Minor applications are typically included as part of a general support system.

Mobile Code: Software programs or parts of programs obtained from remote information systems, transmitted across a network, and executed on a local information system without explicit installation or execution by the recipient.

Multi-factor Authentication: Authentication using two or more factors to achieve authentication. Factors include:

(i) Something you know (e.g., password/PIN);

(ii) Something you have (e.g., cryptographic identification device, token); or

(iii) Something you are (e.g., biometric).

Nonrepudiation: Protection against an individual falsely denying having performed a particular action. Provides the capability to determine whether a given individual took a particular action such as creating information, sending a message, approving information, or receiving a message.

Operational Technology: The use of computers to monitor or alter the physical state of a system, such as the control system for a power station or the control network for a rail system. The term is established to demonstrate the technological and functional differences between traditional IT systems and Industrial Control Systems environment.

Password: A string of characters (letters, numbers, and other symbols) used to authenticate an identity or to verify access authorization.

Patch: An update to an operating system, application, or other software issued specifically to correct particular problems with the software.

Patch Management: The systematic notification, identification, deployment, installation, and verification of operating system and application software code revisions. These revisions are known as patches, hot fixes, and service packs.

Payment Card Industry (PCI) Data Security Standard (DSS) Information: PCI DSS applies to the transmission, storage, or processing of confidential credit card data. This data classification includes credit card magnetic stripe data, card verification values, payment account numbers, personally identification numbers, passwords, and card expiration dates.

Penetration Testing: A test methodology in which assessors, using all available documentation (e.g., system design, source code, manuals) and working under specific constraints, attempt to circumvent the security features of an information system.

Personal Information: New Jersey Revised Statutes § 56:8-161 (2013) defines Personal Information as an individual's first name (or first initial) and last name linked with any one or more of the following data elements: (1) Social Security number; (2) driver's license number or State identification card number; or (3) account number or credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account. Dissociated data that, if linked, would constitute personal information is personal information if the means to link the dissociated data were accessed in connection with access to the dissociated data.

Personally Identifiable Information (PII): NIST Special Publication (SP) 800-121 defines PII as any information about an individual maintained by an organization, including:

(i) Any information that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, or biometric records; and

(ii) Any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information.

Examples of PII include, but are not limited to, the following:

- Name, such as full name, maiden name, mother's maiden name, or alias;
- Personal identification number, such as social security number (SSN), passport number, driver's license number, taxpayer identification number, patient identification number, and financial account or credit card number;
- Address information, such as street address or email address;
- Asset information, such as Internet Protocol (IP) or Media Access Control (MAC) address or other host-specific persistent static identifier that consistently links to a particular person or a smaller, well defined group of people;
- Telephone numbers, including mobile, business, and personal numbers;
- Personal characteristics, including photographic image (especially of the face or other distinguishing characteristics), x-rays, fingerprints, or other biometric image or template data (e.g., retina scan, voice signature, facial geometry);
- Information identifying personally owned property, such as vehicle registration number or title number and related information; and
- Information about an individual that is linked or linkable to one of the above (e.g., date of birth, place of birth, race, religion, weight, activities, geographical indicators, employment information, medical information, education information, financial information).

Personal Identification Number (PIN): A password consisting only of decimal digits.

Personal Information (PI): An individual's first name, or first initial, and last name linked with any one or more of the following data elements:

(i) Social Security number;

(ii) Driver's license number or State identification card number;

(iii) Account number or credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account; or

(iv) Dissociated data that, if linked, would constitute personal information is personal information if the means to link the dissociated data were accessed in connection with access to the dissociated data.

Phishing: A digital form of social engineering that uses authentic-looking—but bogus—emails to request information from users or direct them to a fake Web site that requests information.

Plaintext: Unencrypted information.

Portable Storage Device: An information system component that can be inserted into and removed from an information system, to store data or information (e.g., text, video, audio, and/or image data). Such components are typically implemented on magnetic, optical, or solid-state devices (e.g., floppy disks, compact/digital video disks, flash/thumb drives, external hard disk drives, and flash memory cards/drives that contain non-volatile memory).

Privacy: Freedom from unauthorized intrusion or disclosure of information about an individual or entity.

Privileged Account: An information system account with approved authorizations of a privileged user. (Source: CNSSI-4009; NIST SP 800-53)

Privileged User: A user that is authorized (and, therefore, trusted) to perform security-relevant functions that ordinary users are not authorized to perform.

Process: A structured set of activities designed to accomplish a specific objective.

Protocol: Set of rules and formats, semantic and syntactic, permitting information systems to exchange information.

Remediation: The act of correcting a vulnerability or eliminating a threat.

Remote Access: Access to an organizational information system by a user (or an information system acting on behalf of a user) communicating through an external network (e.g., the Internet).

Risk: The level of impact on organizational operations (including mission, function, image, or reputation), organizational assets, or individuals resulting from the operation of an information system given the potential impact of a threat and the likelihood of that threat occurring.

Risk Assessment: The process of identifying risks to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, and other organizations, arising through the operation of an information system. Part of risk management incorporates threat and vulnerability analyses and considers mitigations provided by security controls planned or in place. Synonymous with risk analysis.

Risk Management: The process of managing risks to organizational operations (including mission, functions, image, and reputation), organizational assets, individuals, other organizations, and the Nation, resulting from the operation of an information system, and includes:

(i) Conducting a risk assessment;

(ii) Implementing risk mitigation strategy; and

(iii) Employing techniques and procedures for the continuous monitoring of the security of information system(s).

Risk Mitigation: Prioritizing, evaluating, and implementing the appropriate risk-reducing controls/countermeasures recommended from the risk management process.

Risk Tolerance: The level of risk an entity is willing to assume in order to achieve a potential desired result.

Role-Based Access Control (RBAC): A model for controlling access to resources where permitted actions on resources are identified with roles rather than with individual subject identities.

Safeguards: Protective measures prescribed to meet the security requirements (i.e., confidentiality, integrity, and availability) specified for an information system. Safeguards may include security features, management constraints, personnel security, and security of physical structures, areas, and devices. Synonymous with security controls and countermeasures.

Sanitization: Process to remove information from media such that information recovery is not possible. It includes removing all labels, markings, and activity logs.

Scanning: Sending packets or requests to another system to gain information to be used in a subsequent attack.

Security: A condition that results from the establishment and maintenance of protective measures that enable an enterprise to perform its mission or critical functions despite risks posed by threats to its use of information systems. Protective measures may involve a combination of deterrence, avoidance, prevention, detection, recovery, and correction that should form part of the enterprise's risk management approach.

Security Controls: The management, operational, and technical controls (i.e., safeguards or countermeasures) prescribed for an information system to protect the confidentiality, integrity, and availability of the system and its information.

Security Requirements: Requirements levied on an information system that are derived from applicable laws, Executive Orders, directives, policies, standards, instructions, regulations, procedures, or organizational mission/business case(s) needs to ensure the confidentiality, integrity, and availability of the information being processed, stored, or transmitted.

Sensitive Authentication Data: Security-related information (including, but not limited to, card validation codes/values, full track data of the magnetic stripe or equivalent on a chip, PINs, and PIN blocks) used to authenticate cardholders and/or authorize payment card transactions.

Sensitive Data: Data that is private, personal, or proprietary and must be protected from unauthorized access.

Sensitive Personally Identifiable Information (SPII): Personal information that, if lost, compromised, or disclosed without authorization, could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual.

Separation of Duties: Practice of dividing steps in a function among different individuals, so as to keep a single individual from being able to subvert the process.

Social Security Administration Provided Information: Information that is obtained from the Social Security Administration (SSA). This can include a Social Security number verification indicator or other PII data.

Stakeholder: Anyone who has a responsibility for, an expectation from, or some other interest in the enterprise.

Strong Cryptography: Cryptography based on industry-tested and accepted algorithms, along with key lengths that provide a minimum of 112-bits of effective key strength and proper key-management practices. Cryptography is a method to protect data and includes both encryption and hashing. Examples of industry-tested and accepted standards and algorithms include: AES (128 bits and higher), TDES/TDEA (triple-length keys), RSA (2048 bits and higher), ECC (224 bits and higher), and DSA/D-H (2048/224 bits and higher).

Strong Password: A minimum of eight characters using a combination of upper and lowercase letters, numbers and special characters.

Supervisory Control and Data Acquisition (SCADA): A control system architecture that uses computers, networked data communications, and graphical user interfaces for high-level process supervisory management, but uses other peripheral devices, such as programmable logic controllers and discrete PID controllers, to interface to the process plant or machinery.

Supply Chain: A system of organizations, people, activities, information, and resources, possibly international in scope that provides products or services to consumers.

System: A discrete set of information technologies (including computer hardware, software, databases, etc.) organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.

System Development Life Cycle (SDLC): The scope of activities associated with a system, encompassing the system's initiation, development and acquisition, implementation, operation and maintenance, and ultimately its disposal that instigates another system initiation.

Third Party: Any entity that an organization does business with. This may include suppliers, vendors, contract manufacturers, business partners and affiliates, brokers, distributors, resellers, and agents. Third parties can be 'upstream' (suppliers and vendors), 'downstream' (distributors and re-sellers), as well as non-contractual parties.

Threat: Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, or other organizations through an information system via unauthorizedaccess, destruction, disclosure, modification of information, and/or denial of service.

Trustworthiness: The attribute of a person or organization that provides confidence to others of the qualifications, capabilities, and reliability of that entity to perform specific tasks and fulfill assigned responsibilities.

Unauthorized Access: Occurs when a user, legitimate or unauthorized, accesses a resource that the user is not permitted to use.

Unauthorized Disclosure: An event involving the exposure of information to entities not authorized access to the information.

User: An individual, or system process acting on behalf of an individual, authorized to access an information system.

User-ID: Unique symbol or character string used by an information system to identify a specific user.

Vulnerability: Weakness in an information system, system security procedure(s), internal controls, or implementation that could be exploited or triggered by a threat source.

Vulnerability Scan: An automated process to proactively identify security weaknesses in a network or individual system.