AEP Security Supplement

This Security Supplement ("Supplement") to the contract or agreement it is attached to (the "Contract") is and in addition to the terms and conditions of the Contract.

This Supplement applies to any Contractor/Seller owned, managed or controlled system, service, application, software, hardware, person or company may store, process, transmit or have access to AEP information or a facility, system or technology which may impact the integrity, availability or confidentiality of AEP information or its systems, or the integrity or availability of the power grid.

This Supplement is intended to establish accountability for maintenance of good security practices within the Contractor/Seller operations, reducing the likelihood of an event that may impact the Contractor/Seller and AEP.

In this Supplement, the following capitalized glossary terms shall have the meaning ascribed next to them as follows and are **specific** to AEP, or as otherwise defined herein:

GLOSSARY

Application Inventory System - An asset based approach that includes an itemized list of applications or application components such that software versions, security testing results and additional attributes can be individually identified against such assets.

Application Vulnerability Assessments/Ethical Hacking - A practice used to identify and treat the validity of vulnerabilities within a product or network with the intent to resolve identified vulnerabilities and increase the stability and security of the product.

Confidential Information – Any confidential or proprietary information, whether written, oral, or visual, whether or not it constitutes a trade secret under applicable law, not specifically marked as "AEP Public."

Data – Information provided by AEP or any resultant data derived from information provided by AEP.

Data Owner – The person with primary responsibility to ensure confidentiality, integrity, and availability of information necessary to operate their business and who determines the sensitivity and controls necessary to protect the information. This person is typically not responsible for the implementation of any of the controls necessary to protect the information.

Data Security Policy – The information security policy that relates to the storage, transmission, and sharing of Confidential Information and Personally Identifiable Information (PII).

Industry Standard Practices – A practice, method, process, or criteria adopted as convention by industry members either through formal agreement or through emulation of best practices established by industry leaders.

Intrusion Detection Systems (IDS) – A system used to identify and analyze activity and compare the results against known attack types. If an attack type is suspected, an alert can be generated to notify responsible parties of the possible attack. An Intrusion Detection System does not stop the attack from occurring.

Intrusion Prevention Systems (IPS) - A system used to identify and analyze activity and compare the results against known attack types. If an attack type is suspected, an alert can be generated to notify responsible parties of the possible attack and block the suspicious activity if it is configured to do so.

NERC CIP Regulated Assets/Information - AEP's identified BES Cyber Assets, Electronic Access Controls or Monitoring Systems, Physical Access Control Systems, and BES Cyber System Information, each as defined in the NERC Glossary of Terms (Glossary_of_Terms.pdf (nerc.com).

Network - Wired and wireless devices and the connecting wires, airwaves, protocols, or other technical mechanisms utilized to facilitate the movement of information and commands from one device or location to another.

Personally Identifiable Information (PII) - An individual's first name or first initial, and last name, in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted: Social Security number; driver's license number; state or Federal government issued ID (in lieu of a driver's license); credit card number; passport number; biometric data (such as, fingerprints, voiceprints, retina or iris images); and/or or bank account or debit card number, along with any required security or password required for access. Personal Identifiable Information shall also have the meaning attributed to it under any applicable data protection law in any relevant jurisdiction.

Privacy Policy – A statement or legal document used to specify how a party may gather, use, disclose, and manage Confidential Information and Personally Identifiable Information (PII).

Security Incident – An event or series of events which indicate potential access to or use of resources by unauthorized person or through unauthorized means.

Systems Development Life Cycle (SDLC) - Referred to as the application development life-cycle, means a process for planning, creating, testing, and deploying an information system.

System – Any device which transmits, processes, stores or interacts with Confidential Information, Data, Personally Identifiable Information (PII), or other AEP devices.

Unrelated Security Incident – An event or series of events in an unauthorized manner and purpose that has compromised the cybersecurity and/or Confidential Information of products/services and while not directly involving products/ services provided to AEP are of a nature that would concern the general cybersecurity of the Contractor/Seller or impact the product or service line utilized by AEP.

AEP Security Supplement

Contractor/Seller has and shall at all times maintain and comply with, and will procure personnel or third-parties who are required to comply with, documented policies and procedures sufficient to maintain the security of AEP Data, including the Confidential Information and related Systems during the term of the Contract to the extent which it applies to the services or work product provided by Contractor/Seller to AEP, as follows:

A. Risk Management

Contractor/Seller must create, maintain, and follow a continuous process for Information Technology (IT) and infrastructure risk management designed to identify, quantify, and prioritize risks against defined risk acceptance levels and objectives relevant to the organization.

A.1 IT and Infrastructure Risk Governance

Contractor/Seller's risk management program must include a formal program, which documents the organization's assets and threats, and evaluates associated risks.

A.2 IT and Infrastructure Risk Assessment Lifecycle

Contractor/Seller's risk management program must examine and evaluate risk within the context of the overall workings of the business and its IT environment.

B. Information Security Policy

Contractor/Seller must provide management direction, and support for information security, in accordance with Contractor/Seller's business requirements, and relevant laws and regulations directing specific security practices. They must set a clear policy direction in line with business objectives and demonstrate support for, and commitment to information security through the issuance, acceptance and maintenance of an information security policy across the organization.

These requirements are designed to reduce the likelihood of an operations impacting event either at the Contractor/Seller facilities or through the Contractor/Seller products and services supplied to AEP under the Contract.

B.1 Information Security Policy Content and Maintenance

Contractor/Seller must establish a security policy that sets the security tone for the whole organization which is reviewed, at least annually, to ensure continued suitability, adequacy, and effectiveness.

B.2 Vendor Management Program

Contractor/Seller must establish, maintain, and follow a documented policy and procedure as part of its overall information security program to manage and assess risk from its third parties. This must include processes that encompass risk ranking, risk assessment, and remediation of risks.

B.2.1 Service Provider Agreements

Contractor/Seller must implement processes designed to ensure that all agreements or contracts with their service provider(s) contain specific clauses to protect Data or Systems when accessed, processed or stored by the service provider.

C. Organization of Information Security

Contractor/Seller must establish, maintain, and follow a management framework to control and manage the information security organization. This framework must include provisions related to the protection of the organization's data in its service provider contracts or agreements as well as outline the roles and responsibilities of those who are responsible for the organization's information security.

C.1 Security Organization Roles and Responsibilities

Contractor/Seller must define, document and maintain well-constructed organization-wide information security roles and responsibilities.

C.2 Security Organization Reporting and Hierarchy Compliance

Contractor/Seller must ensure that the organizational-wide hierarchy is established and maintained in compliance with its internal roles and responsibilities document.

C.3 Data Management

Contractor/Seller must not transfer, store, process, or allow access to AEP Data in, through, to, or from any facility, System, or person outside of the Continental United States without prior explicit written consent of AEP. If, in any case, AEP Data is transferred, stored, processed, or accessed outside of the Continental United States, a written plan must first be submitted by the Contractor/Seller, which includes detailed information about the extent of the AEP Data that will be accessed and how this AEP Data will be accessed. This plan requires prior written approval signed by AEP before any AEP Data can be transferred, stored, processed, or accessed in the manner described in the Contractor/Seller's proposed plan.

C.3.1 Contractor/Seller must notify AEP in writing, no less than 30 business days prior to any change in control of AEP Data that would be in contradiction to Section C.3 of this Supplement.

D. Asset Management

Contractor/Seller must implement, maintain, and follow a formalized asset management program, which includes a process for documenting and maintaining an inventory of hardware, software, and information assets. The documentation relevant to each asset must include an organizational owner who is responsible for the asset throughout its lifecycle.

These requirements are designed to reduce the likelihood of an operations impacting event either at the Contractor/Seller facilities or through the Contractor/Seller products and services supplied to AEP under the Contract by increasing knowledge of the assets in place within the Contractor/Sellers IT environment.

D.1 Asset Accounting and Inventory

Contractor/Seller must implement processes designed to ensure IT assets are clearly identified and an inventory of all IT assets is documented and maintained.

D.2 Asset Destruction

Contractor/Seller must ensure that effective processes and procedures are in place and followed for the destruction of data, media, and assets.

E. Human Resource Security

Contractor/Seller must establish, maintain and follow formal policies for human resources security for employees, as well as any contractors and subcontractors who will access, store, process or transmit AEP Data, including the requirement to conduct appropriate and allowable background screening, acknowledgement of the organization's privacy, information security and risk policies, and periodic formalized training on these policies. Regardless of whether any work operations are completed remotely, Contractor/Seller, as well as all of Contractor/Seller's employees, contractors, and subcontractors, are responsible for making sure that all reasonably necessary security precautions are in place to prevent any foreseeable vulnerabilities that might be associated with remote access to AEP Data.

E.1 Security Awareness Training Attendance

Contractor/Seller must provide security awareness training, which must include at a minimum phishing awareness training, at the time of hire and at least annually thereafter, and maintain attendance records.

E.2 Security Awareness Training Maintenance

Contractor/Seller must review the contents of its security awareness training program at least annually to ensure it is updated and contains recent and relevant IT security information. If any level of work operations are being completed remotely, this security awareness training must also include training specific to secure remote access of information, systems, and data.

E.3 Agreements for Employees

Contractor/Seller's acceptable use, code of conduct/ethics, non-disclosure, and confidentiality agreements must be identified, documented, and implemented. Additionally, employees of the organization must signify acceptance of the same, minimally at the time of hire, and as appropriate thereafter.

E.4 Security Program Management and Communication

Contractor/Seller must maintain and follow a formal information security program to be communicated to all employees, as well as contractors, and subcontractors who will access, store, process or transmit AEP Data, or access AEP Systems or networks, in a relevant, accessible, and understandable format to address compliance with security provisions and address threats and risks.

Contractor/Seller must have an established set of procedures to ensure employees, contractors and subcontractors, if applicable, promptly report actual or suspected breaches of security.

F. Physical and Environmental Security

Contractor/Seller must take all reasonable measures to secure and defend its Systems and facilities from unauthorized physical access or intrusion, as well as accidental and intentional damage to the Contractor/Seller's physical premises, Systems, and information. Contractor/Seller must also take steps intended to protect against environmental and systems malfunctions or failures. Regardless of whether any work operations are completed remotely, Contractor/Seller, as well as all of Contractor/Seller's employees, contractors, and subcontractors, are responsible for making sure that all reasonably necessary physical and environmental security precautions are in place to prevent any foreseeable vulnerabilities that might be associated with remote access of AEP Data.

F.1 Environmental Controls

Contractor/Seller must implement processes designed to ensure critical supporting utilities, such as climate control, fire suppressants and backup power supplies needed to support the business are in place and functional.

F.2 Physical Security Controls

Contractor/Seller must develop processes designed to ensure a formal physical access policy and restrictive controls are established, maintained, and followed. Formal procedures designed to control the allocation of physical access rights to the organization's facilities must also be in place.

F.3 Secure Workspace Security Program

Contractor/Seller must implement processes designed to ensure protecting the secure workspace environment is part of their security and risk management program. Such processes shall include but not be limited to, securing all devices utilized to access AEP Data.

F.4 Secure Workspace Perimeter

Contractor/Seller must implement processes designed to control ingress and egress to and from the secure workspace. The level of controls must be commensurate with the level of risk.

F.5 Secure Workspace Access Reporting

Contractor/Seller must maintain access and incident reports in accordance with Contractor/Seller's internal policies and standards, for a minimum of 90 days.

F.6 Secure Workspace Compliance Audit

Contractor/Seller must complete and document periodic internal or external compliance audits to ensure the workspace environment remains secure. For Contractor/Seller's employees, contractors, and subcontractors who are working remotely are assessed utilizing multifactor authentication with Cisco Umbrella on all corporate devices to ensure secure access to all project data stored.

G. Communications and Operations Management

Contractor/Seller must maintain and follow documented operating procedures and technological controls to ensure the effective management, operation, integrity, and security of Contractor/Seller's information systems and data.

G.1 Network Security – IDS/IPS Signature Updates

Contractor/Seller must implement, maintain, and follow processes designed to ensure that Intrusion Detection Systems (IDS)/Intrusion Prevention Systems (IPS) are maintained to effectively monitor and respond to the most recent threats and vulnerabilities.

G.1.1 Network Security – IDS/IPS Attributes

Contractor/Seller must ensure that IDS/IPS Systems have been deployed, that alerts contain sufficient information to evaluate a potential incident, and that they are generating active alerts.

G.2 Network Security – Firewall(s)

Contractor/Seller Networks must be segregated with the intent of protecting Systems and applications from threats. This must include utilizing firewalls to segment and protect the organization's internal network from the Internet, and also from other less restricted internal Networks.

G.3 Network Management – Encrypted Authentication Credentials

Contractor/Seller must implement processes designed to protect credentials as they travel through the Network. To prevent possible exposure of credentials, an organization must ensure Systems have encryption enabled for network authentication.

G.4 Open Ports

Contractor/Seller must manage open ports and disable those that are not specifically required for business functionality. This is particularly relevant for administrative ports that can be used to manage a system.

G.5 Network Logging

Contractor/Seller must implement, maintain, and follow processes designed to monitor and log activities of its Networks and Systems, and ensure appropriate logging and monitoring are applied to enable recording of relevant actions. Any and all VPN systems or software must be logged to document failed and successful connections; source and destination of connections; connection time; and identity used to make the connection.

G.6 Malware Protection

Contractor/Seller must implement, maintain, and follow measures and processes designed to ensure malware protection is deployed on information assets, and that these are maintained to protect against current IT threats.

G.7 Administrative Activity Logging

Contractor/Seller must implement, maintain, and follow processes designed to comply with all relevant security requirements applicable to its monitoring and logging activities, and ensure that appropriate logging and monitoring of its Systems is in place to capture administrative activity for accountability and audit purposes.

G.8 Log-on Activity Logging

Contractor/Seller must implement, maintain, and follow processes designed to ensure that log-on and log-off attempts to its systems and/or devices are captured and stored for accountability and audit requirements.

G.9 Log Retention

Contractor/Seller must implement, maintain, and follow processes designed to ensure that system and network logs are retained for a sufficient period of time to allow for the successful auditing of historical events and/or to meet legal requirements; or preserved as relevant evidence for forensic investigation purposes in accordance with Contractor/Sellers relevant policies.

G.10 Website Privacy Policy

Contractor/Seller must have a Privacy Policy developed, published, and clearly communicated. This policy must be accessible to all who access the Contractor/Seller's Internet-facing end-user websites that have or which may allow access to Confidential Information, or PII.

G.11 Website – Client encryption

Contractor/Seller must implement processes designed to ensure Confidential Information, or PII transmitted between websites and clients remains confidential and protected from unauthorized disclosure as well as message alteration.

G.12 Email Security

Contractor/Seller must ensure sufficient steps are taken to secure privileged access and prevent misuse of its email resources. For any cloud-enabled email service, multi-factor authentication must be enabled.

G.13 Physical Media Tracking

Contractor/Seller must ensure processes and procedures are in place and functional which are designed to protect and handle, storage and transport of external media (flash drive, media cards, hard drives, etc.), including physical documents, containing Confidential Information, or PII, from unauthorized access, modification and/or disclosure.

G.14 Unapproved Wireless Networks

Contractor/Seller must implement processes designed to ensure all of its Network connections and devices are adequately tracked, managed and controlled to protect against threats and to maintain security for the systems and applications using the Network. Contractor/Seller must have the most recent security controls and firmware in place for the Network.

G.15 Wireless Networks Encryption

Contractor/Seller must implement processes designed to ensure wireless encryption for authorized wireless access points to protect from threats, and to maintain security for the systems and applications using the Network. Minimum requirements for encryption include the following: cryptographic methods (hash functions, symmetric key algorithms, or asymmetric key algorithms) and primitives (e.g., Secure Hash Algorithm [SHA]- 256, Advanced Encryption Standard [AES]-128, RSA, and Digital Signature Algorithm [DSA]-2048) that are implemented in the system, and how these methods are to be implemented.

G.16 Network Security – Authorized Network Traffic

Contractor/Seller must implement processes to verify each network service permitted has been formally approved and authorized.

G.17 Restoration of Data and Systems

Contractor/Seller must have systems, applications, and data available in the event of a disaster. Backups of these systems and data must be maintained, and they must contain copies of original data. Restoration of data (error free and in its original state) must be tested periodically.

G.18 Change Control

Contractor/Seller must implement processes designed to ensure changes are managed within a formal change control program.

G.19 Data Security Policy – Encryption

Contractor/Seller must establish a Data Security Policy designed to ensure Confidential Information, and PII remains confidential and protected from unauthorized disclosure or alteration.

G.20 Data Retention

Unless an alternate timeframe is specifically addressed within this Supplement or any Contract, whenever this Supplement requires Contractor/Seller to retain records, without limitation: Contractor/Seller shall destroy all AEP information at AEP's request, but in any event following completion of the applicable services provided under the Contract except to the extent: (a) required by U.S. law; (b) expressly required or permitted by AEP in writing; (c) to the extent necessary to comply with AEP's or Contractor/Seller's legal or regulatory obligations; or (d) as otherwise permitted in accordance with the Contract. Electronic media that is not physically destroyed must be irrevocably erased or degaussed, such that the media is no longer readable for any purpose. Contractor/Seller must develop and document information destruction processes that meet Industry Standard Practices and must be used in all cases when AEP information is no longer needed. Contractor/Seller shall keep records of all AEP information destruction completed and provide such records to AEP upon demand.

H. Access Control

Contractor/Seller shall develop and implement policies and procedures to address the security of remote and onsite access to Data, Systems and Networks, and AEP property.

H.1 Logical Access Authorization

Contractor/Seller must implement processes designed to ensure a formal user registration and approval procedure, to which employees consistently adhere, is in place for granting access to all systems. Formal procedures designed to control the allocation of logical access rights to systems must be in place.

H.2 Logical Access Authentication

Contractor/Seller shall ensure access to Internet hosted Systems, and Systems, application or platforms offered as a service, is provisioned, and managed in accordance with Industry Standard Practices, to include the use of multi-factor authentication for office (including hybrid and remote) automation products or email services.

H.3 Password Controls

Contractor/Seller must implement processes designed to ensure its password controls align with Industry Standard Practices and follow internal policies, where applicable. Passwords used to access AEP Data and systems must be at a minimum at least eight characters long and include the following: (i) lowercase letter(s), (ii) uppercase letter(s), (iii) numbers, and (iv) special character(s).

H.4 Revoke System and Physical Access

If Contractor/Seller employee, contractor, or subcontractor has access to NERC CIP Regulated Assets/Information, Contractor/Seller will terminate such access within 24 hours of the Contractor/Seller employee, contractor, or subcontractor no longer requiring such access, and/or if Contractor/Seller employee, contractor, or subcontractor has access to AEP Networks, Data, or Systems, Contractor/Seller will notify AEP in writing at **TPRG@AEP.COM**, within 24 hours of termination or change of status of any of the above as set forth below, and will take all steps necessary to remove Contractor/Seller employee's, contractor's and subcontractor's access to any AEP Data, Systems, Networks, or property under Contractor/Seller's control or any Contractor/Seller Data, Systems, or Networks (notification to AEP not necessary for access termination to Contractor/Seller's assets) when:

H.4.1 any Contractor/Seller employee, contractor and subcontractor if applicable, no longer requires such access in order to furnish the services or products provided by Contractor/Seller under the Contract,

H.4.2 any Contractor/Seller employee, contractor and subcontractor if applicable, is terminated or suspended or his or her employment is otherwise ended,

H.4.3 Contractor/Seller reasonably believes any Contractor/Seller employee, contractor and subcontractor if applicable, poses a threat to the safe working environment at or to any AEP property, including to employees, customers, buildings, assets, Systems, Networks, trade secrets, confidential data, and/or employee or Data,

H.4.4 there are any material adverse changes to any Contractor/Seller employee's, contractor's and subcontractor's (if applicable) background history, including, without limitation, any information not previously known or reported in his or her background report or record,

H.4.5 any Contractor/Seller employee, contractor and subcontractor if applicable, fails to maintain conduct in accordance with the qualification criteria set forth in Contractor/Seller or AEP policies and standards,

H.4.6 any Contractor/Seller employee, contractor and subcontractor if applicable, loses his or her U.S. work authorization, or

H.4.7 Contractor/Seller's provision of products and services to AEP under the Contract is either completed or terminated, so that AEP can discontinue electronic and/or physical access for such Contractor/Seller employee, contractor, and subcontractor if applicable.

H.5 Denial of Access and Retrieval of Property

When Contractor/Seller accesses; has or uses AEP owned or managed facilities or assets, Contractor/Seller will take all steps reasonably necessary to immediately deny such Contractor/Seller employees, contractors and subcontractors, if applicable, electronic and physical access to Data as well as AEP property, Systems, or Networks, including, but not limited to, removing and securing individual credentials and access badges, RSA tokens, and laptops, as applicable, and will return to AEP any AEP-issued property including, but not limited to, AEP photo ID badge, keys, parking pass, documents, or laptop in the possession of such Contractor/Seller employees, contractors and subcontractors. Contractor/Seller will notify AEP at **TPRG@AEP.COM** once access to Data as well as AEP property, Systems, and Networks has been removed. All physical equipment owned by AEP, must be returned to AEP, in good working order, within 30 calendar days, or Contractor/Seller shall be responsible for reimbursing the cost of such equipment.

H.6 Authority Over Access

In the course of furnishing products and services to AEP under the Contract, Contractor/Seller shall not access, and shall not permit its employees, agents, contractors, and other personnel or entities within its control (Contractor/Seller employees, contractors, and subcontractors, if applicable) to access AEP's property, Systems, Networks or Data without AEP's prior express written authorization. Such written authorization may subsequently be revoked by AEP at any time in its sole discretion. Further, any Contractor/Seller employee, contractor, and subcontractor if applicable, access shall be consistent with, and in no case exceed the scope of, any such approval granted by AEP. All AEP authorized connectivity or attempted connectivity to AEP's Systems or Networks shall be in conformity with AEP's security policies as may be amended from time to time with notice to the Contractor/Seller.

H.7 Contractor Review of Access

Contractor/Seller will review and verify Contractor/Seller employees, contractors and subcontractors if applicable, continued need for access and level of access to Data; and Systems, Networks and property on a semi-annual basis and will retain evidence of the reviews for two years from the date of each review.

H.8 Controls for Unattended Systems

Contractor/Seller must implement processes designed to ensure sufficient preventative controls, such as screen or session timeouts, are in place to prevent unauthorized access to unattended systems. All devices that can be used to access AEP Data or systems must be locked at any time that they are not being actively used or have been left unattended to make sure that access to the data and systems is secure. Additionally, there must be timeout procedures in place for these systems to ensure that no additional access is permitted after the given time period.

H.9 Multifactor Authentication for Remote Access

Contractor/Seller must utilize multifactor authentication designed to provide an additional level of security for employees, contractors and subcontractors with remote access to Contractor/Seller Systems.

I. Information Systems Acquisition, Development and Maintenance

Contractor/Seller must utilize a comprehensive application security program designed to help ensure applications, both internal and third party, are consistent with Industry Standard Practices and commercially reasonable security requirements. This must include full application compliance testing and software development reviews, as applicable.

I.1 Obligation to Track and Report Vulnerabilities

In the event Contractor/Seller provides AEP with any product containing or consisting of digital and/or third-party components, Contractor/Seller represents and warrants that the Contractor/Seller has a lot tracking system in place such that Contractor/Seller is able to identify and report security vulnerabilities in the product, regardless of whether the product was manufactured or furnished by the Contractor/Seller or a third party). Contractor/Seller shall report any vulnerabilities to AEP within thirty (30) calendar days of discovery by notifying AEP at **TPRG@AEP.COM**.

I.2 Application Vulnerability Assessments/Ethical Hacking

Contractor/Seller must perform application penetration tests or ethical hacking of proprietary applications. Industry Standard Practices or other authoritative sources must be utilized as a foundation for detecting vulnerabilities in the applications, and measuring the effectiveness of the application security controls in place. Vulnerabilities identified must be tracked and remediated in accordance with a defined plan and Contractor/Seller's internal policies. If the vulnerability is in a product provided to AEP as a part of the Contract, the defined plan must be agreed upon by AEP and Contractor/Seller.

I.3 Vulnerability Identification, Management, and Notification

Contractor/Seller shall develop and implement policies and procedures to address the disclosure and remediation by Contractor/Seller of vulnerabilities and material defects related to the products and services provided to AEP under the Contract including the following:

I.3.1 Prior to the delivery of the procured product or service, Contractor/Seller shall provide summary documentation of publicly disclosed vulnerabilities and material defects related in the procured product or services, the potential impact of such vulnerabilities and material defects, the status of Contractor/Seller's efforts to mitigate those publicly disclosed vulnerabilities and material defects, and Contractor/Seller's recommended corrective actions, compensating security controls, mitigations, and/or procedural workarounds.

I.3.2 Contractor/Seller shall provide summary documentation of vulnerabilities and material defects in the procured product or services within thirty (30) calendar days after such vulnerabilities and material defects become known to Contractor/Seller. by notifying AEP at **TPRG@AEP.COM**. This includes summary documentation on vulnerabilities that have not been publicly disclosed or have only been identified after the delivery of the product. The summary documentation shall include a description of each vulnerability and material defects and its potential impact, root cause, and recommended corrective actions, compensating security controls, mitigations, and/or procedural workarounds.

I.3.3 Contractor/Seller shall disclose the existence of all known methods for bypassing computer authentication in the procured product or services, often referred to as backdoors, and provide written documentation that all such backdoors created by Contractor/Seller have been permanently deleted or disabled by notifying AEP at **TPRG@AEP.COM**.

I.3.4 Contractor/Seller shall implement a vulnerability detection and remediation program. The program must include process (es) for identifying and addressing vulnerabilities in any third party products or frameworks used in the development of products covered by the Contract.

I.3.5 Contractor/Seller must notify AEP of vulnerabilities in products provided or hosted by them specifically related to fulfillment of the Contract, which may impact confidentiality, integrity, or availability of Data. Notifications must be sent to **TPRG@AEP.COM**.

I.4 Disclosure of Vulnerabilities by Company

Whether or not publicly disclosed by Contractor/Seller and notwithstanding any other limitation in the Contract, AEP may disclose any vulnerabilities or material defects which may impact the stability and reliability to the power grid or cause harm to entities utilizing the products and services provided by Contractor/Seller to (a) the Electricity Information Sharing and Analysis Center, the Industrial Control Systems Cyber Emergency Response Team, or any equivalent entity, (b) to any entity when necessary to preserve the reliability of Systems as determined by AEP in its sole discretion, or (c) any entity required by applicable law.

I.5 Secure Systems Development Lifecycle (SDLC) Code Reviews

Contractor/Seller's Systems Development Life Cycle (SDLC) must include security Industry Standard Practices within the key development phases of code, where applicable.

I.6 Secure System Hardening

Contractor/Seller must ensure that a formal, documented configuration standard exists for building and managing Systems. This must include key configuration and hardening requirements in accordance with security Industry Standard Practices, to reduce the risk of compromise.

I.7 System Patching

Contractor/Seller must implement a software update management process designed to ensure the most relevant, current, Contractor/Seller approved updates are installed for all authorized software. This process must also include weighing the benefit associated with installing an update to resolve vulnerability against other factors, including the potential impact to system stability and methods to verify authenticity of the source of the code and integrity of the code after delivery.

I.8 Hardware, Firmware, Software, and Patch Integrity and Authenticity

Contractor/Seller shall establish, document, and implement risk management practices for supply chain delivery of hardware, software (including patches), and firmware provided under the Contract. Contractor/Seller shall upon request provide documentation on its: chain-of-custody practices, inventory management program (including the location and protection of spare parts), information protection practices, integrity management program for components provided by sub-suppliers, instructions on how to request replacement parts, commitment to ensure that for as long as the product is supported by the Contractor/Seller, spare parts shall be made available by Contractor/Seller.

I.8.1 Contractor/Seller shall specify how digital delivery for procured products (e.g., software and data) including patches will be validated and monitored to ensure the digital delivery remains as specified. If AEP deems that it is warranted, Contractor/Seller shall apply encryption to protect procured products throughout the delivery process.

I.8.1.1 If Contractor/Seller provides software or patches to AEP, Contractor/Seller shall publish or provide a hash conforming to the Federal Information Processing Standard (FIPS) Security Requirements for Cryptographic Modules (FIPS 140-2) or similar standard information on the software and patches to enable AEP to use the hash value as a checksum to independently verify the integrity of the software and patches and avoid downloading the software or patches from Contractor/Seller's website that has been surreptitiously infected with a virus or otherwise corrupted without the knowledge of Contractor/Seller.

I.8.2 Contractor/Seller shall identify the country (or countries) of origin of the procured product and its components (including hardware, software, and firmware). Contractor/Seller will identify the countries where the development, manufacturing, maintenance, and service for the product are provided. Contractor/Seller will notify AEP of changes in the list of countries where product maintenance or other services are provided in support of the procured product. This notification shall occur 180 days prior to initiating a change in the list of countries by notifying AEP at **AEP@TPRG.COM**.

I.8.3 Contractor/Seller shall use trusted channels to ship procured products, such as U.S. registered mail.

I.8.4 Contractor/Seller shall demonstrate chain-of-custody documentation for procured products as determined by AEP in its sole discretion and require tamper-evident packaging for the delivery of this hardware.

I.9 Software and Hardware Bill of Materials (SBOM and HBOM)

Contractor/Seller must provide a full list of all components used to develop any software or hardware product provided to AEP prior to its delivery to AEP, and must include the source of development, manufacture, and assembly of those components. Product source must include whether the component is externally or internally developed and/or the component is developed utilizing open source code.

I.9.1 Foreign Ownership, Control, or Influence (FOCI)

Contractor/Seller must disclose any foreign ownership, control, or investment in their parent companies or subsidiaries. Disclosure must include country of involvement, percentage of investment, and amount of influence from the foreign participant. An annual certification must be submitted regarding any FOCI in Contactor/Seller business. Certification must be sent to: **TPRG@AEP.COM**.

I.9.2 Attestation of No Banned Products/ Relationships in Scope of Product and/or Service

Contractor/Seller attests that no banned products and/or relationships are included in the scope of products and services provided to AEP. Banned entities are to include, but not limited to the National Defense Authorization Act (NDAA) 889 and (NDAA) 1237 et. al, and Executive Order 13971 of January 5, 2021 (Addressing the Threat Posed by Applications and Other Software Developed or Controlled by Chinese Companies) (“EO 13971”).

I.10 Patching Governance

Prior to the delivery of any products and services to AEP or any connection of electronic devices, assets or equipment to AEP’s electronic equipment, Contractor/Seller shall provide documentation regarding its patch management and vulnerability management/mitigation programs and update process (including third-party hardware, software, and firmware) for products, services, and any electronic device, asset, or equipment required to be connected to the assets of AEP during the provision of products and services under the Contract. This documentation shall be sent to **TPRG@AEP.COM** and include information regarding:

I.10.1 the resources and technical capabilities to sustain this program and process such as Contractor/Seller’s method or recommendation for how the integrity of a patch is validated by AEP; and

I.10.2 Contractor/Seller's approach and capability to remediate newly reported zero-day vulnerabilities.

I.11 Out of Date Components

Unless otherwise approved by AEP in writing, current or supported version of Contractor/Seller products and services shall not require the use of an out-of-date, unsupported, or end-of-life version of third-party components (e.g., Java, Flash, Web browser, etc.). Additionally, other out of date systems or applications may not be supported by AEP. To access AEP Data and Systems, the Contractor/Seller’s operation system, applications, and products must be properly updated and maintained.

I.12 Software and Firmware Updates

Contractor/Seller shall verify and provide documentation that procured products (including third-party hardware, software, firmware, and services) have appropriate updates and patches installed prior to delivery to AEP.

I.12.1 In providing the products and services described in the Contract, Contractor/Seller shall provide appropriate software and firmware updates to remediate newly discovered vulnerabilities or weaknesses within 30 days. Updates to remediate critical vulnerabilities shall be provided within a shorter period than other updates, within 7 days. If updates cannot be made available by Contractor/Seller within these time periods, Contractor/Seller shall provide mitigations and/or workarounds within no greater than 30 days. Required notification must be sent to AEP at **TPRG@AEP.COM** in accordance with the preceding required timelines.

I.12.2 When third-party hardware, software (including open-source software), and firmware is provided by Contractor/Seller to AEP, Contractor/Seller shall provide appropriate hardware, software, and firmware updates to remediate newly discovered vulnerabilities or weaknesses within 30 calendar days. Updates to remediate critical vulnerabilities shall be provided within a shorter period than other updates, within 7 calendar days. If these third-party updates cannot be made available by Contractor/Seller within these time periods, Contractor/Seller shall provide mitigations and/or workarounds within 15 calendar days. Required notification must be sent to AEP at **TPRG@AEP.COM** in accordance with the preceding required timelines.

I.13 Viruses, Firmware and Malware

Contractor/Seller will use reasonable efforts to investigate whether computer viruses or malware are present in any software or patches before providing such software or patches to AEP.

I.13.1 Contractor/Seller warrants that it has no knowledge of any computer viruses or malware coded or introduced into any software or patches, and Contractor/Seller will not insert any code which would have the effect of disabling or otherwise shutting down all or a portion of such software or damaging information or functionality.

I.13.2 When install files, scripts, firmware, or other Contractor/Seller delivered software solutions are flagged as malicious, infected, or suspicious by an anti-virus vendor through open source solutions like “Virus Total,” Contractor/Seller must provide technical proof as to why the “false positive” hit has taken place to ensure their code’s supply chain has not been compromised.

I.13.3 If a virus or other malware is found to have been coded or otherwise introduced as a result of Contractor/Seller’s breach of its obligations under this Supplement, Contractor/Seller shall immediately and at its own cost:

I.13.3.2 Take all necessary remedial action and provide assistance to AEP to eliminate the virus or other malware throughout AEP's information networks, computer systems, and information systems, regardless of whether such systems or Networks are operated by or on behalf of AEP; and

I.13.3.3 If the virus or other malware causes a loss of operational efficiency or any loss of data (A) where Contractor/Seller is obligated under this Supplement to back up such data, take all steps necessary and provide all assistance required by AEP and its affiliates, and (B) where Contractor/Seller is not obligated under this Supplement to back up such data, use commercially reasonable efforts, in each case to mitigate the loss of or damage to such data and to restore the efficiency of such data.

I.13.4 End of Life Operating Systems

Contractor/Seller delivered solutions will not be required to reside on end-of-life operating systems, or any operating system that will go end-of-life six (6) months from the date of installation.

I.13.4.1 Contractor/Seller solutions will support the latest versions of operating systems on which Contractor/Seller-provided software functions within twenty-four (24) months from official public release of that operating system version.

I.14 Cryptographic Requirements

Contractor/Seller shall document how the cryptographic system protects the confidentiality, data integrity, authentication, and non-repudiation of devices and data flows in the underlying system as specified by the Contract. This documentation shall include, but not be limited to, the following:

I.14.1 The cryptographic methods (hash functions, symmetric key algorithms, or asymmetric key algorithms) and primitives (e.g., Secure Hash Algorithm [SHA]- 256, Advanced Encryption Standard [AES]-128, RSA, and Digital Signature Algorithm [DSA]-2048) that are implemented in the system, and how these methods are to be implemented.

I.14.2 The preoperational and operational phases of key establishment, deployment, ongoing validation, and revocation.

I.14.3 An automated remote key-establishment (update) method that protects the confidentiality and integrity of the cryptographic keys

I.14.4 Contractor/Seller shall ensure that:

I.14.4.2 The system implementation includes the capability for configurable cryptoperiods (the life span of cryptographic key usage) in accordance with the Suggested Cryptoperiods for Key Types found in Table 1 of NIST 800-57 Part 1, as may be amended.

I.14.4.3 The key update method supports remote re-keying of all devices within 72 hours as part of normal system operations.

I.14.4.4 Emergency re-keying of all devices can be remotely performed within 24 hours.

I.14.5 Contractor/Seller shall provide a method for updating cryptographic primitives or algorithms.

I.15 Application Security Program Governance

Contractor/Seller must manage application development activities, methodologies, and application security risk. Application security must be part of Contractor/Seller's overall risk governance framework.

I.16 Application Security Vulnerability Assessment and Response

Contractor/Seller must ensure application security vulnerabilities are assessed for business risk and impact, and have a vulnerability response plan.

I.17 Application Security SDLC Phases

Contractor/Seller must implement processes designed to ensure security requirements are part of the key phases of their internal SDLC program. This process must be designed to ensure that security reviews, security scans, and security signoff occur at applicable phases.

I.18 Application Security Awareness Training Content

Contractor/Seller must implement processes designed to ensure the content of its application security awareness program incorporates current and relevant security attack and vulnerability mitigation, and that the course content is applicable to the organization and its environment.

I.19 Application Security Awareness Training Attendance

Contractor/Seller must implement processes designed to ensure its software developers are aware of application security and secure coding practices and that they complete a formal, Industry Standard based application security training program at least annually.

I.20 Secure Software Delivery

Contractor/Seller must provide a means for verification, by AEP of authenticity of source, and integrity of all software, patches, and firmware received by AEP from Contractor/Seller.

I.21 Security Review of Internal and External Applications

Contractor/Seller must perform security reviews of applications developed internally, as well as third party applications that process, store, or transmit Data.

J. Security Incident Response and Management

Contractor/Seller shall develop and implement policies and procedures to address security incidents ("**Response Plan**") by mitigating the harmful effects of security incidents and addressing and remedying the occurrence to prevent the recurrence of security incidents in the future. Contractor/Seller shall provide AEP access to inspect its Response Plan.

Any and all notifications required in this Section J will be made within 24 hours of identification to the AEP Cybersecurity Intelligence and Response Center at 1-866-747-5845; OR, by encrypted email at **INCIDENTS@AEP.COM**, and follow-up in writing to AEP Cybersecurity, ATTN: Cyber Intelligence and Response Center, 1 Riverside Plaza, 4th Floor, Columbus, Ohio 43215, unless otherwise specified in the Supplement or the Contract.

J.1 Security Incident Notification

Immediately upon learning of a security incident related to the products and services provided to AEP, Contractor/Seller shall implement its Response Plan and, within 24 hours of implementing its Response Plan, shall notify AEP of that implementation.

J.1.1 The notice shall include the date and time of the Security Incident occurrence (or the approximate date and time of the occurrence if the actual date and time of the occurrence is not precisely known) and a detailed summary of the facts and circumstances of the Security Incident, including a description of (a) why the Security Incident occurred (e.g., a precise description of the reason for the system failure), (b) the amount of Data known or reasonably believed to have been disclosed, and (c) the measures being taken to address and remedy the occurrence to prevent the same or a similar event from occurring in the future.

J.1.2 Contractor/Seller shall provide written updates, through encrypted email to **INCIDENTS@AEP.COM** of the notice to AEP addressing any new facts and circumstances learned after the initial written notice is provided and shall provide such updates within a reasonable time after learning of those new facts and circumstances. Contractor/Seller shall cooperate with AEP in AEP's efforts to determine the risk to AEP Systems posed by the Security Incident, including providing additional information regarding the Security Incident upon request from Contractor/Seller by AEP.

J.2 Notification to Affected Parties

Contractor/Seller will, at its sole cost and expense, assist and cooperate with AEP with respect to disclosures to affected parties, and other remedial measures as requested by AEP and agreed upon by both parties, in connection with a Security Incident or required under any applicable laws related to a Security Incident.

J.2.1 In the event a Security Incident results in Data being disclosed such that notification is required to be made to any person or entity, including without limitation any customer, shareholder, or current or former employee of AEP under any applicable laws, including privacy and consumer protection laws, or pursuant to a request or directive from a governmental authority, such notification will be provided by AEP, except as required by applicable law or approved by AEP in writing. AEP will have sole control over the timing and method of providing such notification, unless otherwise specifically mandated by law or regulation.

J.3 Prevention of Recurrence

Within 30 days of a Security Incident, Contractor/Seller shall develop and execute a plan that reduces the likelihood of the same or a similar Security Incident from occurring in the future consistent with the requirements of its Response Plan and NIST Special Publication 800-61 Rev. 2 and NIST Special Publication 800-184, as may be amended, and shall communicate that plan to AEP. Contractor/Seller shall provide recommendations to AEP on actions that AEP may take to assist in the prevention of recurrence, as applicable or appropriate.

J.4 Coordination of Incident Response

Within 3 calendar days of notifying AEP of the Security Incident, Contractor/Seller shall recommend actions to be taken by AEP on AEP-controlled Systems, where AEP Systems are running, hosting or connected to contractor/seller products, Networks, or services, to reduce the risk of a recurrence of the same or a similar Security Incident, including, as appropriate, the provision of action plans and mitigating controls. Contractor/Seller shall coordinate with AEP in developing those action plans and mitigating controls. Contractor/Seller will provide AEP guidance and recommendations for long term remediation of any cyber security risks posed to Data, equipment, Systems, and Networks as well as any information necessary to assist AEP in any recovery efforts undertaken by AEP in response to the Security Incident.

J.5 Unrelated Security Incidents

In the event Contractor/Seller receives any complaint, notice, communication, or knows that an act or omission has compromised their cybersecurity and/or Confidential Information has been corrupted, destroyed, accessed, acquired, compromised, modified, used, or disclosed by any unauthorized person, or by any person in an unauthorized manner or for an unauthorized purpose in compliance with applicable law, Contractor/Seller shall provide to AEP a confidential report describing, to the extent legally permissible, a summary of the facts and circumstances of the Unrelated Security Incident promptly; however, no later than 7 calendar days of identification of the event.

K. Business Continuity Management

Contractor/Seller must incorporate business continuity considerations into the overall design of their business model to mitigate the risk of service disruptions and the impacts of those within the supply chain. This must include an enterprise-wide, process-oriented approach that considers technology, business operations, testing, and communication strategies that are critical to business continuity planning for the entire business.

K.1 Business Impact Analysis

Contractor/Seller must conduct an assessment of and prioritize all business functions and processes, including their interdependencies, as part of a workflow analysis. This assessment must also evaluate the potential impact of business disruptions resulting from uncontrolled, non-specific events on the organization's business functions and processes.

K.2 Threat Assessment

Contractor/Seller must create and maintain an in-depth business threat assessment that includes, realistic threat scenarios such as malicious activity, natural and technical disasters, and pandemic incidents. The magnitude of the business disruption must consider a wide variety of threat scenarios, including capacity.

K.3 Business Continuity Governance

Contractor/Seller must create and maintain an in-depth business continuity governance plan that documents the program details, the decision making and communication process, and defines who is responsible for which components of governance.

K.4 Business Insurance

Contractor/Seller must ensure applicable insurance coverages are defined and outlined within their business continuity plan.

K.5 Business Process Level Readiness

Contractor/Seller must create and conduct business continuity planning and analysis to be able to evaluate the business continuity readiness of end-to-end business processes.

K.6 Business Continuity Threat Assessment

Contractor/Seller must create and maintain realistic threat scenarios which consider internal, business partners, and customers. These threat scenarios must focus both on the impact of the threat as well as the nature of the threat.

K.7 Business Continuity Process Testing

Contractor/Seller must create and maintain detailed business continuity test plans. These must include scoping the business process and identifying the dependencies, as well as detailed testing to complete a realistic and thorough test.

L. Technical Compliance Checking

Contractor/Seller must implement procedures that will enable compliance with their legal, regulatory, statutory, and/or contractual obligations related to any information security requirements.

L.1 Vulnerability Testing and Remediation

Contractor/Seller must ensure Contractor/Seller Systems are regularly scanned for compliance against security Industry Standard Practices and other authoritative sources, and that any applicable detected vulnerabilities are addressed.

L.2 For Proprietary Systems or Solutions Provided to AEP

Contractor/Seller agrees that they will use commercially reasonable efforts to identify and notify AEP by email to **TPRG@AEP.COM** of any mitigated or remediated vulnerabilities, risks and threats which impact the confidentiality, integrity or availability of proprietary solutions provided to AEP within 24 hours of the latter, identification or mitigation, and provide guidance as to how the applicable mitigations, patches or remediations are to be deployed.

M. PII Protection

Should Contractor/Seller have access to, process, store, transmit, or manage PII, Contractor/Seller must establish and maintain a privacy program and management framework intended to control and manage the protection of PII. This must include the overall management of PII within the organization and with all third parties. The privacy program must include: individuals responsible for the creation, oversight and maintenance of the program; all third parties meeting their commitments under the organization's business requirements, applicable privacy laws, policies, processes, technologies, and industry leading practices; and the protection and privacy of PII through its lifecycle of collection, storage, usage, processing, sharing, transferring, securing, retention and destruction.

M.1 PII Inventory and Flows

Contractor/Seller must maintain an inventory of PII that must, at a minimum, define PII by data subject category or data classification based on the data inventory, assign ownership for PII, and document the flow of PII throughout the data lifecycle of collection, storage, usage processing, sharing, trans-border flows, retention and retirement though the organization. The inventory must include all PII that is provided to, or shared with, any of the organizations affiliates, subcontractors, or other third parties.

M.2 Privacy Policy and Privacy Notices

Contractor/Seller must provide management policy, direction, and support for information privacy in accordance with its legal, regulatory, and contractual obligations to provide privacy protection for PII. It must demonstrate support for, and commitment to, information privacy through the issuance, acceptance and maintenance of internal privacy policies across the organization. It must, where required, communicate that commitment to data subjects via external privacy notices and where applicable, gain their consent and seek their permission for certain uses of PII (e.g., protected PII). It must ensure that third parties' privacy policies and privacy notices are consistent with its privacy policies and privacy notices. The privacy policies and privacy notices must incorporate the key areas of privacy and must be reviewed at planned intervals (at least annually), or if significant changes occur, to ensure continuing suitability, adequacy and effectiveness.

M.3 Privacy Organization and Program Maintenance

Contractor/Seller must implement processes designed to ensure the service provider and its applicable third parties each have a designated privacy function responsible for its privacy policy and program as it relates to PII. The privacy program must contain enforcement and monitoring procedures and a change management procedure to remain current with privacy changes in business requirements, applicable privacy law, policy, and industry best practices.

M.4 Third Party Privacy Agreements

Contractor/Seller must ensure agreements with third parties contain specific clauses to ensure PII is protected and that certain other privacy requirements are included, where those third parties access, process or store PII.

M.5 Legal Authorizations

Contractor/Seller and its third parties that access, process or store PII must have completed the applicable notifications, registrations, permit, approvals, and/or adequacy derogations as required by applicable law.

M.6 Management of PII

Contractor/Seller must implement processes designed to ensure collection, storage, use, access, sharing, transport, retention and deletion of PII is in accordance with applicable law, Privacy Policy, privacy notices, and Industry Standard Practices, and is represented in their documented procedures, and that these procedures are maintained.

Contractor/Seller must require all third-party contractors and subcontractors who will be engaged by Contractor/Seller and who may impact the integrity, confidentiality or availability of Systems or services provided by Contractor/Seller to AEP, to keep any PII received by Contractor/Seller and disclosed by AEP as confidential for a defined period of time either through the Contract or Contractor/Seller policies and standards.

PII provided to Contractor/Seller must not be allowed outside of the continental United States without expressed written authorization of AEP.

M.7 Privacy Awareness

Contractor/Seller and its third parties must ensure recurring privacy awareness training occurs for their employees and participation records are maintained. This ensures employees are aware of key information privacy requirements and their obligations to maintain the privacy of AEP PII.

M.8 Privacy Incident Notification and Response Management

Contractor/Seller must establish a formal privacy incident communication procedure, integrated with the Information Security Incident Management Program to be executed in the event of unauthorized disclosure or breach or other required privacy communication requirement to data subjects or other entities, including applicable law enforcement and governmental agencies. Contractor/Seller must establish procedures for notification by third parties that access, process, or store PII. These procedures must include the documentation of a post incident report which documents the unauthorized disclosure, breach, lessons learned, and a summary of events related to the incident. Notification to AEP shall be completed in accordance with Section J of this Supplement.

N. Control Laws

Contractor/Seller must comply with all U.S. or other export and import laws and restrictions (the "**Control Laws**") applicable to any commodities, software or technology provided or disclosed in connection with any Service, Work Product, activity, delivery or development hereunder, including any restrictions on the exposure or release of technical data, software source code or other information as that term is contemplated in the Control Laws ("**Information**") to any non-U.S. national personnel, whether located within or outside of the United States. Contractor/Seller must implement, maintain and follow, at all times during the Term of the Contract, appropriate technology control programs and procedures compliant with the Control Laws to prevent the unauthorized exposure or release of Information, including measures that prevent access to Information by non-U.S. national personnel. Contractor/Seller must advise AEP immediately of any violation of a Control Law, must cooperate with AEP in any investigation of an actual or possible violation and must take any measures AEP reasonably may request to rectify or address such violation. Notification must be sent to **TPRG@AEP.COM.**

N.1 Export-Related Information

Contractor/Seller must provide to AEP all export control classification numbers (U.S. ECCNs or foreign equivalents, where applicable), export licenses, advisory opinions, Government Authority classifications, classification requests and commodity jurisdiction requests relating to any commodities, software or technology provided or disclosed in connection with any service, work product, activity, delivery or development under the Contract or any related Statement of Work, and any Government Authority correspondence relating thereto as available and applicable.

N.2 Prohibited Persons

Neither the Contractor/Seller nor any Contractor/Seller employee, contractor or subcontractor if applicable, may appear on any list of prohibited persons maintained by any Government Authority ("**Prohibited Lists**"), including but not limited to the list of "Specially Designated Nationals and Other Blocked Persons" maintained by the United States Department of Treasury, and the "Denied Persons List" maintained by the Bureau of Industry & Security. Contractor/Seller must monitor for changes to the Prohibited Lists and ensure continuing compliance, at least annually. Contractor/Seller must immediately remove from all AEP projects any Contractor/Seller employee, contractor or subcontractor, if applicable identified on a Prohibited List, must immediately inform AEP of same, must cooperate with AEP in any investigation thereof, and must take any measures AEP reasonably may request to rectify or address any violation of applicable law that is discovered.

O. Software Application Security Policies and Standards

If Contractor/Seller utilizes or provides proprietary or customized software to, or for AEP, Contractor/Seller must ensure software security policies, standards and procedures are implemented, maintained, and followed; and that stakeholders, business owners, and internal governing bodies have a common understanding of business practices and risk management expectations. Contractor/Seller must also ensure security controls are employed throughout the Systems Development Lifecycle (SDLC) to confirm secure coding practices are followed as an integral part of the development process.

O.1 Application Inventory

Contractor/Seller must document and maintain an Application Inventory System which will enable security evaluation tracking to specific assets.

O.2 Risk Classification

Contractor/Seller must implement and maintain a risk classification process, which evaluates the level of inherent risk an information resource is exposed to. The risk classification drives the required set of controls that must be implemented. Application risk classifications must be performed annually, for all applications (including third party developed applications) and if any application changes are made the application must be reassessed.

O.3 Secure Architectural Design Standards

Contractor/Seller must have a process in place intended to ensure software applications are designed with secure architecture design standards. These standards must include, but are not limited to, threat modeling or secure application reviews.

O.4 Secure Code Review

Contractor/Seller must ensure secure code reviews are performed prior to promotion to non-development environments in order to identify insecure coding defects.

O.5 Open Source

Contractor/Seller must ensure the use of open source code is documented and maintained in accordance with Industry Standard Practices. Open source code must only be used if it is properly managed. Contractor/Seller will be responsible to ensure any open source content used in the products or services provided to AEP will be maintained, assessed, and remediated for vulnerabilities, flaws or other risks. If the Contractor/Seller cannot ensure the maintenance and/or security of the Open Source content, the Open Source content must be removed from the product delivered to AEP.

O.6 Production Evaluation Process

Contractor/Seller must ensure software applications in production are evaluated in accordance with Industry Standard Practices.

P. Contractor/Seller Fourth Party Controls Management

If the Contractor/Seller will be using subcontractors to provide material services under the Contract, Contractor/Seller must establish, maintain, and follow a documented policy to manage and assess the risk of their own third party's utilization of subcontractors.

P.1 Subcontractor Selection and Management Process

The Contractor/Seller must have a subcontractor selection and management process in place.

P.2 Subcontractor Contracting Process

Contractor/Seller must have contracts in place with all subcontractors who store, process, transmit, manage, or access Data.

P.2.1 Contractor/Seller must not contract with a third-party to provide material services under the Contract, without full disclosure to and prior authorization of AEP.

P.2.2 Contractor/Seller must require all third-party contractors and subcontractors who will be engaged by Contractor/Seller to provide material services, and who may impact the integrity, confidentiality or availability of Systems or services provided by Contractor/Seller to AEP, to abide by the terms and conditions contained in the Contract and this Supplement.

P.3 Documenting Information Security Assessments for Subcontractors

Contractor/Seller must have a documented process in place to address information security assessments and risk as it relates to third party contractors.

P.4 Calculation of Subcontractor Information Security Risk

Contractor/Seller must have a method for calculating information security risk as it relates to subcontractor's products, services, and interactions.

P.5 Information Security Review Process – Tracking and Risk Rating Subcontractor Issues

Contractor/Seller must track open issues that result from their third party subcontractor's information security review process and assign a risk rating to issues.

Q. Cloud Computing/Third Party Hosted Services

Contractor/Seller must have a clear understanding of where any provider and its subsequent relationships, is hosting AEP Data, and the security controls implemented by those providers to ensure all applicable security measures are approved, implemented and maintained, and align with Industry Standard Practices for hosting data.

Q.1 Service and Deployment Models

Contractor/Seller must have an understanding of the type of service model and deployment model utilized to ensure proper documentation of security responsibilities is managed, approved by management, maintained, and followed.

Q.2 Cloud Computing/Third Party Hosted Service Audit Program

Contractor/Seller and their provider(s) must develop, maintain, and follow audit plans which focus on review and management of information security. System security must be reviewed periodically by management to ensure System security policies are being followed.

Q.3 Security Review of Hypervisor Configuration

Contractor/Seller must apply a standardized monitoring process to ensure secure configuration and operational practices are being applied to virtual host systems and hypervisors.

R. Right to Conduct an Assessment

AEP reserves the right to conduct an Assessment for adherence to the terms of this supplement not more than once per year, with not less than 30 days' notice.

An IT Controls Assessment will include Contractor/Seller's completion of a Controls Assessment questionnaire including supporting documentation (such as policies, procedures, diagrams, and third-party audit reports, as applicable). To the extent there are findings from the Assessment, Contractor/Seller will provide a designated representative(s) to discuss the responses thereto and to work with AEP, or its representatives, to design a mutual written remediation plan.

S. Right to Audit

An audit may be conducted upon notification of a breach of the Contractor/Seller's security controls and this audit will not be counted toward the annual total of allowable assessments.

S.1.1 If audit is conducted due to a breach of the Contractor/Seller's security as a result of a failure of the Contractor/Seller to adequately secure its Systems, the Contractor/Seller must be responsible for all their internal costs and expenses arising from a security audit by AEP in reviewing the Contractor/Seller information security practices. Any travel or lodging expenses incurred by AEP will be the responsibility of AEP.

S.1.2 Contractor/Seller must reasonably cooperate with any audit and provide all appropriate documentation at no cost to AEP. Also, where applicable the Contractor/Seller must furnish copies of all relevant third-party audit reports (e.g. SOC 2, or other assessment documents relevant to the security controls covered under the Contract and this Supplement). Any Contractor/Seller documents submitted shall be considered confidential and proprietary.

T. Remediation

T.1 Contractor/Seller will be provided an opportunity within the IT Controls Assessment questionnaire to self-report any remediation timelines for deficiencies identified in its IT controls identified either by the Assessment or the audit. Contractor/Seller agrees that AEP may rely on the self-reported remediation timelines provided by its designated representative(s) and may follow-up with Contractor/Seller on its progress throughout the course of the remediation plan timeline. Additionally, Contractor/Seller agrees that it will remediate any and all security findings identified by AEP, or AEP's representatives, or any industry recognized vulnerability research or assessment organization, within a mutually agreed upon timeline.

T.2 In connection with any AEP evaluation of Contractor/Seller's security, AEP, or AEP's representative, will classify each identified finding as "Critical", "High", "Medium" or "Low" and such classification shall be in AEP's sole and exclusive discretion pursuant to its internal policies and procedures. AEP will, in good faith, consider internal mitigating controls as well as documented Contractor/Seller's mitigating controls when classifying the severity of findings. A written plan will be developed and maintained by Contractor/Seller which reflects the mutually agreed upon timeline, which will include Contractor/Seller's remediation timelines provided within the IT Controls Assessment questionnaire. Progress will be verified by AEP throughout the course of the plan timeline. Failure to meet the agreed upon timeline could be deemed as a breach of the Contract and activate breach clauses in the Contract.

T.3 AEP, or AEP's representatives, may identify findings in connection with AEP's evaluation of Contractor/Seller's even though such findings are not specifically described or covered by this Supplement.

T.3.1 Contractor/Seller's remediation of findings identified by AEP, or AEP's representatives, shall not interpreted to be a waiver of any of Contractor/Seller's obligations contained in this Supplement or any Contract, and AEP does not forego, waive or forfeit any of its rights under this Supplement or any Contract.

T.3.2 Nothing in this section shall be interpreted to preclude AEP to from deciding that the risk of continuing its engagement with the Contractor/Seller is too high and therefore must be terminated.

U. Representation of Information

Contractor/Seller represents and warrants that all (i) written questionnaire responses and support materials furnished and (ii) oral representations made by Contractor/Seller to AEP, or AEP's representatives, in connection with AEP's evaluation of Contractor/Seller's security or any reporting and or disclosure obligations contained in this Supplement are complete and accurate.

V. Mergers and Acquisitions

Contractor/Seller must disclose to AEP any change in control, which for purposes of this Supplement is defined by the sale of more than 50% of Contractor/Seller's stock; a sale of substantially all of the assets and/or a change of the majority of board members of Contractor/Seller. Notice should be sent to **TPRG@AEP.COM**.

W. Notices

All notices required to be given by Contractor/Seller pursuant to this Supplement must be sent in writing to **TPRG@AEP.COM** unless otherwise stated herein. This requirement is not intended to and does not in any way modify the notice requirements under the Contract and is intended to be an additional notice not a replacement of the notice requirements under the Contract.