Universal Service
Administrative Co.

ATTACHMENT 7

SECURITY AND CONFIDENTIALITY PROCEDURES

Security Requirements for IT Acquisition Efforts

This document provides security and privacy requirements for an external information system (USAC- owned and Contractor-operated or Contractor-owned and operated on behalf of USAC), and "Cloud Information Systems". "Cloud Information Systems "includes Infrastructure as a Service ("IaaS"), Platform as a Service ("PaaS"), or Software as a Service ("SaaS"). It also requires the system to be Federal Risk and Authorization Management ("FedRAMP") authorized. The security and privacy requirements are appropriately formatted to allow the respective security and privacy contract language to be placed in-line within a statement of work for each system type. The security and privacy requirements identified in this document will ensure compliance with the appropriate provisions of Federal Information Security Modernization Act of 2014 (FISMA), OMB Circular A-130, and National Institite of Standards and Technology ("NIST") Special Publication ("SP") 800-53, Revision 5 or most recent later revision (hereafter described as NIST 800-53).

External Information Systems – IT Security Requirements

Information systems supporting USAC must meet the minimum security and privacy requirements through the use of security controls in accordance with NIST 800-53, "Security and Privacy Controls for Federal Information Systems and Organizations".

- Contractor shall comply with all applicable Federal Laws and Regulations.
- Contractor shall comply with all applicable Federal Information Processing Standards ("FIPS"). NIST SP (800 Series) and guidance.
- Contractor shall comply with all applicable USAC Policies.
- Contractor shall apply the appropriate set of Low, Moderate, or High impact baseline security controls in NIST 800-53, as determined by USAC based in accordance with FIPS PUB 199, "Standards for Security Categorization of Federal Information and Information Systems".
- NIST 800-53 controls requiring organization-defined parameters (i.e., password change frequency) shall be consistent with USAC specifications.
- Contractor shall use USAC technical guidelines, NIST guidelines, Center for Internet Security ("CIS") guidelines (Level 1), or industry best practice guidelines in hardening their systems.

The following table lists essential controls that must be implemented prior to system operations. Contractor shall make the proposed system and security architecture of the information system available to the USAC Enterprise Architecture and Security for review and approval before commencement of system build (architecture, infrastructure, and code).

Control ID	Control Title	Baseline	USAC Implementation Guidance
AC-2	Account Management	L, M, H	Access to USAC information systems shall be limited to authorized persons whose job responsibilities require their use. Access shall be given through the establishment of a unique account in accordance with USAC System Access Procedures. Information systems, including vendor owned/operated systems on behalf of USAC, shall configure their systems in agreement with USAC Information Security Procedures, NIST guidelines, CIS guidelines (Level 1), or industry best practice guidelines, as deemed appropriate.
AC-17 (3)	Remote Access | Managed Access Control Points	M, H	All remote accesses from internal users/systems to the external information system must be routed through USAC's managed network access control points, subjecting them to security monitoring.
AU-2	Audit Events	L, M, H	Information systems shall implement audit configuration requirements as documented in applicable USAC Information Security Procedures. For technologies where a technical guide and standard does not exist, events from an industry source such as vendor guidance or CIS benchmark, may be used. The configuration must be approved and accepted by the USAC Security.
CM-6	Configuration Settings	L, M, H	Information systems, including vendor owned/operated systems on behalf of USAC, shall configure their systems in agreement with USAC Information Security Procedures, NIST guidelines, CIS guidelines (Level 1), or industry best practice guidelines, as deemed appropriate.
CP-7	Alternative Processing Site	M, H	FIPS PUB 199 Moderate and High impact systems must implement processing across geographically-disparate locations to ensure fault tolerance. Amazon Web Services based architectures must implement a multi-region strategy (multiple availability zones in a single region are not sufficient).

Control ID	Control Title	Baseline	USAC Implementation Guidance
CP-8	Telecom Services	M, H	FIP PUB 199 Moderate and High impact information systems must implement alternate telecom services to support resumption when the primary telecommunications capabilities are unavailable at either the primary or alternate processing or storage sites.
IA-2 (1)	Identification and Authentication (Organizational Users) | Network Access to Privileged Accounts	L, M, H	All information systems shall implement multi-factor authentication and support integration with USAC multi-factor authentication technology for privileged accounts.
IA-2 (2)	Identification and Authentication (Organizational Users) | Network Access to Non-Privileged Accounts	M, H	FIPS PUB 199 Moderate and High impact information systems must implement multi-factor authentication for non-privileged accounts and support integration with USAC multi-factor authentication technology.
IA-7	Cryptographic Module Authentication	L, M, H	The information system shall implement FIPS PUB 140-2 compliant encryption modules for authentication functions. Reference: https://csrc.nist.gov/Projects/Cryptographic-Module-Validation-Program/Validated-Modules
MP-4	Media Storage	M, H	Digital media including magnetic tapes, external/removable hard drives, flash/thumb drives, diskettes, compact disks and digital video disks shall be encrypted using a FIPS PUB 140-2 certified encryption module.

Control ID	Control Title	Baseline	USAC Implementation Guidance
MP-5	Media Transport	M, H	Digital media including magnetic tapes, external/removable hard drives, flash/thumb drives and digital video disks shall be encrypted using a FIPS PUB 140-2 certified encryption module during transport outside of controlled areas.
PL-8	Information Security Architecture	M, H	All information system security architectures must be formally reviewed and approved by USAC's Chief Information Security Officer ("CISO"), during the system develop/design stages of the system development life cycle ("SDLC") and prior to security assessment and authorization.
RA-5	Vulnerability Scanning	L, M, H	All systems must complete weekly operating system (OS) and monthly web application vulnerability scans. The most recent vulnerability scanning results shall be provided to USAC together with the monthly Plan of Actions & Milestones ("POA&M") submission.
SA-22	Unsupported System Components	USAC Required	All systems must be comprised of software and hardware components that are fully supported in terms of security patching for the anticipated life of the system; software must be on USAC's Enterprise Architecture IT Standards List.

Control ID	Control Title	Baseline	USAC Implementation Guidance
SC-8 / SC-8(1)	Transmission Confidentiality and Integrity / Transmission Confidentiality and Integrity | Cryptographic or Alternate Physical Protection	M, H	Implemented encryption algorithms and cryptographic modules shall be FIPS-approved and FIPS PUB 140-2 validated, respectively. o Digital signature encryption algorithms - Reference: https://csrc.nist.gov/Projects/Cryptographic-Algorithm-Validation-Program/Validation/Validation-List/DSA o Block cypher encryption algorithms - Reference: https://csrc.nist.gov/Projects/Cryptographic-Algorithm-Validation-Program/Block-Ciphers o Secure hashing algorithms – Reference: https://csrc.nist.gov/Projects/Cryptographic-Algorithm-Validation-Program/Secure-Hashing Internet accessible Websites shall implement HTTPS Only and HTTP Strict Transport Security (HSTS), reference OMB Memorandum M-15-13.
SC-13	Cryptographic Protection	L, M, H	Implemented encryption algorithms and cryptographic modules shall be FIPS-approved and FIPS PUB 140-2 validated, respectively. o Digital signature encryption algorithms - Reference: https://csrc.nist.gov/Projects/Cryptographic-Algorithm-Validation-Program/Validation/Validation-List/DSA o Block cypher encryption algorithms - Reference: https://csrc.nist.gov/Projects/Cryptographic-Algorithm-Validation-Program/Block-Ciphers o Secure hashing algorithms – Reference: https://csrc.nist.gov/Projects/Cryptographic-Algorithm-Validation-Program/Secure-Hashing
SC-17	PKI Certificates	M, H	Appropriate creation, use, and signing of crypto certs in must be Implemented in accordance with NIST SP 800-32, NIST SP 800-63.

Control ID	Control Title	Baseline	USAC Implementation Guidance
SC-18	Mobile Code	M, H	Information systems, including vendor owned/operated systems on behalf of USAC, requiring mobile code technologies shall be in compliance with USAC acceptable mobile code and mobile code technologies as defined in Information Security Procedure.
SC-22	Architecture and Provisioning for Name / Address Resolution Service	L, M, H	Information systems shall be Domain Name System Security Extensions ("DNSSEC") compliant. Reference OMB Memorandum M-08-23.
SC-28 (1)	Protection of Information at Rest | Cryptographic Protection	USAC required – For systems with Personally Identifiable Information Only	Systems bearing personally identifiable information ("PII") must protect information at rest. At a minimum, fields bearing PII data must be encrypted with field level encryption. Encryption algorithms shall be FIPS-approved; implemented encryption modules shall be FIPS PUB 140-2 validated.
SI-2	Flaw Remediation	L, M, H	All projects and systems must be adequately tested for flaws; all Critical, High, and Moderate risk findings must be remediated prior to go-live. Post go-live, all critical and high vulnerabilities identified must be mitigated within 30 days, all moderate vulnerabilities mitigated within 60 days, and all low/very low vulnerabilities within 90 days.
SI-3	Malicious Code Protection	L, M, H	Information systems, including vendor owned/operated systems on behalf of USAC, shall configure malicious code protection in accordance with USAC Information Security procedure and applicable NIST guidelines.
SI-4	Information System Monitoring	L, M, H	Information systems, including vendor owned/operated systems on behalf of USAC, shall implement monitoring of the information system in accordance with USAC Information Security procedure and applicable NIST guidelines.

Control ID	Control Title	Baseline	USAC Implementation Guidance
SI-10	Information Input Validation	M, H	All system accepting input from end users must validate the input in accordance to industry best practices and published guidelines, and Open Web Application Security Project (“OWASP” Top 10 Web Application Security Vulnerabilities.
AR-2	Privacy Impact and Risk Assessment	See note below	Contractor shall conduct a Privacy Threshold Analysis (“PTA”) and, if applicable, a Privacy Impact Assessment (“PIA”) identifying the categories of information and addressing potential risks to PII. Contractor also shall coordinate with the USAC Privacy Officer concerning these documents.
AR-8	Accounting of Disclosures	See note below	Contractor shall keep an accurate accounting of disclosures of information held in any system of records under its control.
TR-2	System of Records Notices and Privacy Act Statements	See note below.	Contractor shall coordinate with the USAC Privacy Officer to ensure System of Records Notices (“SORN”s) and Privacy Act notices on forms that collect PII are established and kept current.
UL-1	Internal Use	See note below	Contractor shall ensure that PII is shared internally only for the authorized purpose(s) identified in the Privacy Act of 1974 and/or in public notices.
UL-2	Information Sharing with Third Parties	See note below	Contractor shall coordinate with the USAC Privacy Office to ensure PII is shared in accordance with USAC requirements and agreements with third parties.

Note: Privacy controls are not associated with a baseline. Controls are applicable/not applicable based on PII data being collected, stored, or transmitted.

Assessment and Authorization (“A&A”) Activities

The Contractor system/application must have a valid assessment and authorization, known as an Authority to Operate (“ATO”) before going into operation and processing USAC information. The failure to obtain and maintain a valid ATO may result in the termination of the Contract. The system must have a new A&A Activities conducted when there is a significant change to the system's security posture or via continuous monitoring based on USAC Information Security Continuous Monitoring Strategy, which is reviewed and accepted by the USAC CISO.

Assessing the System

1. Contractor shall comply with the A&A requirements as mandated by Federal laws and policies, including making available any documentation, physical access, and logical access needed to support this requirement. The Level of Effort for the A&A is based on the System's FIPS Publication 199 categorization. The contractor shall create, maintain and update the following A&A documentation:
   - System Security Plan ("SSP") completed in accordance with NIST SP 800-18, Revision 1 or the most recent version.
   - Contingency Plan (including Disaster Recovery Plan) completed in accordance with NIST SP 800-34, the most recent version.
   - Contingency Plan Test Report.
   - Incident Response Plan completed in accordance with NIST SP 800-61, "Computer Security Incident Handling Guide" the most recent version.
   - Incident Response Test Report completed in accordance with NIST SP 800-61, "Computer Security Incident Handling Guide" the most recent version.
   - Configuration Management Plan.
   - Plan of Actions & Milestones.
   - Penetration Test Reports documenting the results of vulnerability analysis and exploitability of identified vulnerabilities.
2. At the Moderate impact level and higher, Contractor is responsible for providing an independent Security Assessment/Risk Assessment in accordance with and NIST SP 800-37.
3. Identified gaps between required NIST SP 800-53 controls and Contractor's implementation as documented in the Security Assessment/Risk Assessment report shall be tracked for mitigation in a POA&M document completed in accordance with USAC Security Procedural POA&M Guide. Depending on the severity of the gaps, USAC may require them to be remediated before an ATO is accepted.

Authorization of the System

1. Upon receipt of the documentation (Security Authorization Package ("SAP")) USAC Authorizing Official ("AO") in collaboration the CISO, will render an acceptance decision to:

   - Allow system operation w/out any restrictions or limitations on its operation;
   - Allow system operation w/restriction or limitation on its operation, or;
   - Not allow for operation.

2. TContractor shall provide access to USAC, or their designee acting as their agent, when requested, in order to verify compliance with the requirements for an Information Security Program. At its option, USAC may choose to conduct on site surveys. Contractor shall make appropriate personnel available for interviews and documentation during this review. If documentation is considered proprietary or sensitive, these documents may be reviewed on-site under the hosting Contractor's supervision.

Reporting and Continuous Monitoring

Through continuous monitoring, security controls and supporting deliverables are updated and submitted to USAC per the agreed upon schedule. The submitted deliverables (or lack thereof) provide a current understanding of the security state and risk posture of the information systems. They allow USA AOs to make credible risk-based decisions regarding the continued operations of the information systems and initiate appropriate responses as needed when changes occur.

Cloud Specific Security Requirements

Contractor shall implement the controls contained within the FedRAMP Cloud Computing Security Requirements Baseline and FedRAMP Continuous Monitoring Requirements for <SELECT Low, Moderate, or High> impact systems (as defined in FIPS PUB 199). The Contractor system must be FedRAMP authorized. Contractor shall generally, substantially, and in good faith follow FedRAMP guidelines and security guidance.

Contractor shall comply with FedRAMP requirements as mandated by Federal laws and policies, including making available any documentation, physical access, and logical access needed to support this requirement.

USAC may choose to cancel the Contract and terminate any outstanding orders if Contractor has its FedRAMP authorization (Joint Authorization Board [“JAB”] Provisional or Agency) revoked and the deficiencies are greater than agency risk tolerance thresholds.

USAC will leverage the CSP’s FedRAMP A&A package to document and assess the customer controls for which USAC has responsibility and issue a USAC ATO for the USAC’s instance of the CSP’s SaaS or PaaS offering. The CSP shall work with the USAC to facilitate documentation and assessment of required customer controls, as necessary.

Protection of Information

Contractor shall be responsible for properly protecting all information used, gathered, or developed as a result of work under this contract. Contractor shall also protect all USAC data, equipment, etc. by treating the information in accordance with its FISMA system categorization.

All information about the systems gathered or created under this Contract should be considered as SBU information. If Contractor personnel must remove any information from the primary work area that is included in the ATO boundary, they should protect it to the same security requirements. The use of any information that is subject to the Privacy Act will be utilized in full accordance with all rules of conduct as applicable to Privacy Act Information.

When no longer required, this information, data, and/or equipment shall be returned to USAC control, destroyed, or held until otherwise directed. Destruction of items shall be accomplished by following NIST Special Publication 800-88, “Guidelines for Media Sanitization”.

USAC will retain unrestricted rights to USAC data. The ordering activity retains ownership of any user created/loaded data and applications hosted on vendor’s infrastructure, as well as maintains the right to request full copies of these at any time.

The data must be available to USAC upon request within one business day or within the timeframe negotiated with Contractor, and shall not be used for any other purpose other than that specified herein. Contractor shall provide requested data at no additional cost to USAC.