EXHIBIT E – IT SECURITY CONTROLS

If selected through this RFP process respondent shall provide an initial Security Controls Report in the form attached hereto prior to executing an agreement with LACERA. All subsequent Security Controls Reports that are required after this first report shall be performed and submitted annually. The questionnaires are to focus on security as it applies to the technologies impacting services provided in relation to the scope of work. If a control is found to be inadequate, respondent will develop a remediation plan within 30 days. Respondent will implement the plan and inform LACERA of the change within a mutually agreed upon and reasonable time.

The Security Controls Reports shall report in writing on the respondent's system(s) and the suitability of the design and operating effectiveness of controls, information functions, and/or processes applicable to the environment in which the respondent receives and maintains LACERA records, including the security requirements.

Respondent shall provide to LACERA, within 30 calendar days of the issuance of each Security Controls Report, a documented corrective action plan that addresses each audit finding or exception contained therein. The corrective action plan shall show in detail the required remedial action by respondent along with the implementation date(s) for each remedial action.

If respondent does not obtain an annual Security Controls Report, LACERA shall have the right to retain an independent audit firm to perform such an audit engagement for such a report. The audit will include the controls, information functions, and processes used or provided by respondent. Respondent agrees to allow the independent audit firm to access its facilities for purposes of conducting this audit engagement. They will provide the necessary support and cooperation to the independent audit firm.

The independent audit firm will be engaged by LACERA's legal department and subject to the same confidentiality requirements supported in this agreement, and any disclosure will be on a need-to-know basis only for the purpose of the Security Controls Report. LACERA will invoice respondent for the expense of the report(s) or deduct the cost from future payments to the respondent.

Control Identifier	Control Name	LACERA Supply Chain IT Security Controls Assessment Control Description	Has the Control Been Tested and Validated?	Validation Results or Location of Documented Results
LACERA-0		LACERA Conducts supplier assessment of risk prior to the acquisition or outsourcing of information Systems, Security Services; and will verify that the acquisition or outsourcing of dedicated information security services is approved by the CISO.		
LACERA-1	Supplier	Legal Name of Supplier		
LACERA-2	Supplier	Legal form of business (e.g., U.S. Corporation)		
LACERA-3	Supplier	Parent Corporation		
LACERA-4	Supplier	Web Site		
LACERA-5	Supplier	Dun & Bradstreet Number		
LACERA-6	Supplier	U.S. Federal Taxpayer ID		
LACERA-7	Supplier	What percentage of product/service - development/support is off-shore (non-U.S.)		
LACERA-8	Supplier	What is Supplier's 3rd-Party Security Assessment Validation (e.g., ISO, 27001:13, SOC 2 Type 2)		
LACERA-8	Supplier	Is your product FIPS 140-2 or 140-3 Certified (if yes, provide cert #)		
AC-1	Policy and Procedures	Are Access Control Policy(s) supported		
AC-2(1)	Account Management	Are System Accounts / Service Accounts / Privileged Accounts supported or required		
AC-2(3)	Account Management | Disable Accounts	Documented procedure or automated tool to Disable accounts		
AC-2(4)	Account Management | Automated Audit Actions	Automatic logging for audit of account creation, modification, enabling, disabling, and removal actions.		
AC-2(5)	Account Management | Inactivity Logout	Automatically log out users when [defined time period of inactivity].		

Control Identifier	Control Name	LACERA Supply Chain IT Security Controls Assessment Control Description	Has the Control Been Tested and Validated?	Validation Results or Location of Documented Results
AC-2(12)	Account Management | Account Monitoring for Atypical Usage	(a) Monitor / log system accounts login; and (b) Report usage of system accounts to [actions].		
AC-3(7)	Access Enforcement | Role-based Access Control	Enforce a role-based access control policy over defined subjects and objects and control access based upon [defined roles and users authorized to assume such roles].		
AC-3(9)	Access Enforcement | Controlled Release	Release information outside of the system only if: (a) The receiving [destination] provides [authentication]; and (b) [user roles] are used to validate the appropriateness of the information designated for release.		
AC-3(11)	Access Enforcement | Restrict Access to Specific Information Types	Restrict access to data repositories containing [Customer-defined information types].		
AC-3(12)	Access Enforcement | Assert and Enforce Application Access	(a) Require integration / API applications to use validated certificates. (c) Validate access changes after initial installation of the application.		
AC-3(14)	Access Enforcement | Individual Access	Provide [mechanisms] to enable individuals (Subjects) to have access to [defined elements] of their personally identifiable information.		
AC-4	Information Flow Enforcement	Enforce approved authorizations for controlling the flow of information within the system and between connected systems based on [defined information flow control policies].		
AC-4(2)	Information Flow Enforcement | Processing Domains	Use protected processing domains to enforce [defined information flow control policies] as a basis for flow control decisions.		
AC-4(5)	Information Flow Enforcement | Embedded Data Types	Enforce [defined limitations] on embedding data types within other data types.		

Control Identifier	Control Name	LACERA Supply Chain IT Security Controls Assessment Control Description	Has the Control Been Tested and Validated?	Validation Results or Location of Documented Results
AC-4(11)	Information Flow Enforcement | Configuration of Security or Privacy Policy Filters	Provide the capability for privileged administrators to configure [defined] security or privacy policy filters to support different security or privacy policies.		
AC-4(26)	Information Flow Enforcement | Audit Filtering Actions	When transferring information between different security domains, record and audit content filtering actions and results for the information being filtered.		
AC-6(6)	Least Privilege | Privileged Access by Non-organizational Users	Prohibit privileged access to the system by non-organizational users.		
AC-6(9)	Least Privilege | Log Use of Privileged Functions	Log the execution of privileged functions.		
AC-6(10)	Least Privilege | Prohibit Non-privileged Users from Executing Privileged Functions	Prevent non-privileged users from executing privileged functions.		
AC-7	Unsuccessful Logon Attempts	Enforce a limit of [defined number] consecutive invalid logon attempts by a user during a [organization-defined time period]; and automatically lock the account for an [organization-defined time period] or lock the account until released by an administrator and notify system administrator when the maximum number of unsuccessful attempts is exceeded.		
AC-8	System Use Notification	a. Display system use notification message or banner to users before granting access to the system		
AC-12(2)	Session Termination | Termination Message	Display an explicit logout message to users indicating the termination of authenticated communications sessions.		
AC-12(3)	Session Termination | Timeout Warning Message	Display an explicit message to users indicating that the session will end in [defined time until end of session].		

Control Identifier	Control Name	LACERA Supply Chain IT Security Controls Assessment Control Description	Has the Control Been Tested and Validated?	Validation Results or Location of Documented Results
AC-14	Permitted Actions Without Identification or Authentication	a. Identify [user actions] that can be performed on the system without identification or authentication; and b. Document and provide supporting rationale in the security plan for the system, user actions not requiring identification or authentication.		
AC-16(10)	Security and Privacy Attributes | Attribute Configuration by Authorized Individuals	Provide authorized individuals the capability to define or change the type and value of security and privacy attributes available for association with subjects and objects.		
AC-24	Access Control Decisions	Establish procedures; Implement mechanisms to ensure [access control decisions] are applied to each access request prior to access enforcement.		
AU-2	Event Logging	a. Identify the types of events that the system is capable of logging in support of the audit function		
AU-3	Content of Audit Records	Ensure that audit records contain information that establishes the following: a. What type of event occurred; b. When the event occurred; c. Where the event occurred; d. Source of the event; e. Outcome of the event; and f. Identity of any individuals, subjects, or objects/entities associated with the event.		
AU-9(2)	Protection of Audit Information | Store on Separate Physical Systems or Components	Store audit records in a repository that is part of a physically different system or system component than the system or component being audited.		
AU-9(3)	Protection of Audit Information | Cryptographic Protection	Implement cryptographic mechanisms to protect the integrity of audit information and audit tools.		

Control Identifier	Control Name	LACERA Supply Chain IT Security Controls Assessment Control Description	Has the Control Been Tested and Validated?	Validation Results or Location of Documented Results
AU-11	Audit Record Retention	Retain audit records for [organization-defined time period consistent with records retention policy] to provide support for after-the-fact investigations of incidents and to meet regulatory and organizational information retention requirements.		
CM-3(2)	Configuration Change Control | Testing, Validation, and Documentation of Changes	Test, validate, and document changes to the system before finalizing the implementation of the changes.		
CM-14	Signed Components	Prevent the installation of [software and firmware components] without verification that the component has been digitally signed using a certificate that is recognized and approved by the organization.		
CP-4(4)	Contingency Plan Testing | Full Recovery and Reconstitution	Include a full recovery and reconstitution of the system to a known state as part of [Organization]contingency plan.		
CP-9(8)	System Backup | Cryptographic Protection	Implement cryptographic mechanisms to prevent unauthorized disclosure and modification of backup information.		
CP-10	System Recovery and Reconstitution	Provide for the recovery and reconstitution of the system to a known state within recovery time and recovery point objectives after a disruption, compromise, or failure.		
CP-10(2)	System Recovery and Reconstitution | Transaction Recovery	Implement transaction recovery for systems that are transaction-based.		
CP-10(4)	System Recovery and Reconstitution | Restore Within Time Period	Provide the capability to restore system components from configuration-controlled and integrity-protected information representing a known, operational state for the components.		
CP-10(6)	System Recovery and Reconstitution | Component Protection	Protect system components used for recovery and reconstitution.		

Control Identifier	Control Name	LACERA Supply Chain IT Security Controls Assessment Control Description	Has the Control Been Tested and Validated?	Validation Results or Location of Documented Results
IA-2(1)	Identification and Authentication (organizational Users) | Multi-factor Authentication to Privileged Accounts	Implement multi-factor authentication for access to privileged accounts.		
IA-2(2)	Identification and Authentication (organizational Users) | Multi-factor Authentication to Non-privileged Accounts	Implement multi-factor authentication for access to non-privileged accounts.		
IA-2(5)	Identification and Authentication (organizational Users) | Individual Authentication with Group Authentication	When shared accounts or authenticators are employed, require users to be individually authenticated before granting access to the shared accounts or resources.		
IA-2(8)	Identification and Authentication (organizational Users) | Access to Accounts — Replay Resistant	Implement replay-resistant authentication mechanisms for access to [Selection (one or more): privileged accounts; non-privileged accounts]. Techniques used to address this include protocols using nonces (e.g., numbers generated for a specific one-time use) or challenges (e.g., TLS, WS_Security) and PKI certificates. Additional techniques include time-synchronous or challenge-response one-time authenticators.		
IA-2(10)	Identification and Authentication (organizational Users) | Single Sign-on	Provide a single sign-on capability for system accounts and services.		
IA-2(12)	Identification and Authentication (organizational Users) | Acceptance of PIV Credentials	Accept and electronically verify Personal Identity Verification-compliant credentials.		

Control Identifier	Control Name	LACERA Supply Chain IT Security Controls Assessment Control Description	Has the Control Been Tested and Validated?	Validation Results or Location of Documented Results
IA-4(1)	Identifier Management | Prohibit Account Identifiers as Public Identifiers	Prohibit the use of system account identifiers that are the same as public identifiers for individual accounts.		
IA-5(1)	Authenticator Management | Password-based Authentication	For password-based authentication: (a) Maintain a list of commonly-used, expected, or compromised passwords and update the list when organizational passwords are suspected to have been compromised directly or indirectly; (b) Verify, when users create or update passwords, that the passwords are not found on the list of commonly-used, expected, or compromised passwords in IA-5(1)(a); (c) Transmit passwords only over cryptographically-protected channels; (d) Store passwords using an approved salted key derivation function, preferably using a keyed hash; (e) Require immediate selection of a new password upon account recovery; (f) Allow user selection of long passwords and passphrases, including spaces and all printable characters; (g) Employ automated tools to assist the user in selecting strong password authenticators.		
IA-5(2)	Authenticator Management | Public Key-based Authentication	(a) For public key-based authentication: (1) Enforce authorized access to the corresponding private key; and (2) Map the authenticated identity to the account of the individual or group; and (b) When public key infrastructure (PKI) is used: (1) Validate certificates by constructing and verifying a certification path to an accepted trust anchor, including checking certificate status information; and (2) Implement a local cache of revocation data to support path discovery and validation.		

Control Identifier	Control Name	LACERA Supply Chain IT Security Controls Assessment Control Description	Has the Control Been Tested and Validated?	Validation Results or Location of Documented Results
IA-5(5)	Authenticator Management | Change Authenticators Prior to Delivery	Require developers and installers of system components to provide unique authenticators or change default authenticators prior to delivery and installation.		
IA-5(7)	Authenticator Management | No Embedded Unencrypted Static Authenticators	Ensure that unencrypted static authenticators are not embedded in applications or other forms of static storage.		
IA-7	Cryptographic Module Authentication	Implement mechanisms for authentication to a cryptographic module that meets the requirements of AT LEAST FIPS -140-2.		
IA-8(2)	Identification and Authentication (non-organizational Users) | Acceptance of External Authenticators	(a) Accept only external authenticators that are NIST-compliant; and (b) Document and maintain a list of accepted external authenticators.		
IR-4(5)	Incident Handling | Automatic Disabling of System	Implement a configurable capability to automatically disable the system if [security violations] are detected.		
IR-4(6)	Incident Handling | Insider Threats	Implement an incident handling capability for detecting incidents involving insider threats.		
IR-4(11)	Incident Handling | Integrated Incident Response Team	Establish and maintain an incident response team that can be deployed to any location identified by the organization within [defined time period].		
IR-4(14)	Incident Handling | Security Operations Center	Establish and maintain a security operation [support] center.		
IR-4(15)	Incident Handling | Public Relations and Reputation Repair	(a) Manage public relations associated with an incident; and (b) Employ measures to repair the reputation of the organization.		
IR-5	Incident Monitoring	Track and document incidents.		

Control Identifier	Control Name	LACERA Supply Chain IT Security Controls Assessment Control Description	Has the Control Been Tested and Validated?	Validation Results or Location of Documented Results
IR-5(1)	Incident Monitoring | Automated Tracking, Data Collection, and Analysis	Track [security] incidents and collect and analyze incident information [preferably using automated mechanisms].		
IR-6(3)	Incident Reporting | Supply Chain Coordination	Provide incident information to the customer of the product or service and other organizations involved in the supply chain or supply chain governance for systems or system components related to the incident.		
IR-7	Incident Response Assistance	Provide an incident response support resource, integral to the supplier's organizational incident response capability, that offers advice and assistance to users of the system for the handling and reporting of incidents.		
IR-8	Incident Response Plan	1. Provide the [Customer's] organization with a roadmap for implementing supplier's incident response capability; 2. Describes the structure and organization of the incident response capability; 3. Provides a high-level approach for how the incident response capability fits into the overall organization; 5. Defines reportable incidents; 6. Provides metrics for measuring the incident response capability within the organization; 7. Defines the resources and management support needed to effectively maintain and mature an incident response capability; 8. Addresses the sharing of incident information; 10. Explicitly designates responsibility for incident response.		

Control Identifier	Control Name	LACERA Supply Chain IT Security Controls Assessment Control Description	Has the Control Been Tested and Validated?	Validation Results or Location of Documented Results
IR-8(1)	Incident Response Plan | Breaches	Include the following in the Incident Response Plan for breaches involving personally identifiable information: (a) A process to determine if notice to individuals or other organizations, including oversight organizations, is needed; (b) An assessment process to determine the extent of the harm, embarrassment, inconvenience, or unfairness to affected individuals and any mechanisms to mitigate such harms; and (c) Identification of applicable privacy requirements.		
IR-9	Information Spillage Response	Respond to information spills by: a. Assigning personnel with responsibility for responding to information spills; b. Identifying the specific information involved in the system contamination; c. Alerting [defined personnel or roles] of the information spill using a method of communication not associated with the spill; d. Isolating the contaminated system or system component; e. Eradicating the information from the contaminated system or component; f. Identifying other systems or system components that may have been subsequently contaminated.		
IR-9(3)	Information Spillage Response | Post-spill Operations	Implement procedures to ensure that organizational personnel impacted by information spills can continue to carry out assigned tasks while contaminated systems are undergoing corrective actions.		
MA-2(2)	Controlled Maintenance | Automated Maintenance Activities	(a) Schedule, conduct, and document maintenance, repair, and replacement actions for the system; and (b) Produce up-to date, accurate, and complete records of all maintenance, repair, and replacement actions requested, scheduled, in process, and completed.		
MA-3(2)	Maintenance Tools | Inspect Media	Check media containing diagnostic and test programs for malicious code before the media are used in the system.		
PL-7	Concept of Operations	a. Develop a Concept of Operations (CONOPS) for the system describing how to operate the system from the perspective of information security and privacy; and b. Review and update the CONOPS.		

Control Identifier	Control Name	LACERA Supply Chain IT Security Controls Assessment Control Description	Has the Control Been Tested and Validated?	Validation Results or Location of Documented Results
PL-10	Baseline Selection	Define the security controls baseline for the system.		
PM-2	Information Security Program Leadership Role	Appoint a senior agency information security officer with the mission and resources to coordinate, develop, implement, and maintain an organization-wide information security program.		
PM-3	Information Security and Privacy Resources	a. Include the resources needed to implement the information security and privacy programs in capital planning and investment requests and document all exceptions to this requirement; b. Prepare documentation required for addressing information security and privacy programs in capital planning and investment requests in accordance with applicable laws, executive orders, directives, policies, regulations, standards; and c. Make available for expenditure, the planned information security and privacy resources.		
PM-4	Plan of Action and Milestones Process	a. Implement a process to ensure that plans of action and milestones for the information security, privacy, and supply chain risk management programs and associated organizational systems: 1. Are developed and maintained; 2. Document the remedial information security, privacy, and supply chain risk management actions to adequately respond to risk to organizational operations and assets, individuals, other organizations, and 3. Are reported in accordance with established reporting requirements. b. Review plans of action and milestones for consistency with the organizational risk management strategy and organization-wide priorities for risk response actions.		
PM-7(1)	Enterprise Architecture | Offloading	As a supplier of products / services, are any essential functions or services offloaded to other systems, system components, or an external provider [specify]		

Control Identifier	Control Name	LACERA Supply Chain IT Security Controls Assessment Control Description	Has the Control Been Tested and Validated?	Validation Results or Location of Documented Results
RA-5	Vulnerability Monitoring and Scanning	a. Monitor and scan for vulnerabilities in the system and hosted applications b. Employ vulnerability monitoring tools for: 1. Enumerating platforms, software flaws, and improper configurations; 2. Formatting checklists and test procedures; and 3. Measuring vulnerability impact; c. Analyze vulnerability scan reports and results from vulnerability monitoring; d. Remediate legitimate vulnerabilities; e. Share information obtained from the vulnerability monitoring process		
RA-5(11)	Vulnerability Monitoring and Scanning | Public Disclosure Program	Establish a public reporting channel for receiving reports of vulnerabilities in systems and system components.		
SA-4(1)	Acquisition Process | Functional Properties of Controls	Require the developer of the system, system component, or system service to provide a description of the functional properties of the controls to be implemented.		
SA-4(2)	Acquisition Process | Design and Implementation Information for Controls	The developer of the system, system component, or system service must provide design and implementation information for the controls that includes security-relevant external system interfaces; high-level design; low-level design; source code or hardware schematics;		
SA-4(3)	Acquisition Process | Development Methods, Techniques, and Practices	The developer of the system, system component, or system service must demonstrate the use of a system development life cycle process that includes: (a) Systems engineering methods; (b) Systems security; privacy, engineering methods; and (c) Software development methods; testing, evaluation, assessment, verification, and validation methods; and quality control processes.		
SA-4(5)	Acquisition Process | System, Component, and Service Configurations	The developer of the system, system component, or system service must: (a) Deliver the system, component, or service with security configurations implemented; and (b) Use security configurations as the default for any subsequent system, component, or service reinstallation or upgrade.		

Control Identifier	Control Name	LACERA Supply Chain IT Security Controls Assessment Control Description	Has the Control Been Tested and Validated?	Validation Results or Location of Documented Results
SA-4(12)	Acquisition Process | Data Ownership	Are organizational data ownership requirements in the acquisition contract; and terms that require all data to be removed from the vendor's system and returned to the Customer-organization within [defined time frame].		
SA-9(2)	External System Services | Identification of Functions, Ports, Protocols, and Services	Identify the functions, ports, protocols, and other services required for the use of such services.		
SA-9(8)	External System Services | Processing and Storage Location — U.S. Jurisdiction	Is the geographic location of information processing and data storage facilities located within in the legal jurisdictional boundary of the United States?		
SC-45(1)	System Time Synchronization | Synchronization with Authoritative Time Source	Synchronize the internal system clocks to the authoritative time source within Stratum 3.		

(*The rest of this page is left intentionally blank*)