EXHIBIT B

LAWA Information Security Requirements

LAWA Information Security Requirements

The term 'Information Systems Security' reference in this section refers to an application or operating systems software and hardware to host any component of this proposed solution. The Selected Contractor shall incorporate security best practices and meet a standard of due care to support the security policy of Los Angeles World Airports and shall abide by the following requirements:

A. Security Controls

Selected Contractor shall be responsible for configuring security controls to provide individual accountability, audit ability, and separation of duties. Security controls must be consistent with industry best practices, including but not limited to the following:

- Authentication requirements for access to sensitive data and privileged functions.
- Ensure the latest operating system patches have been applied to all components.
- Ensure the latest security-related patches have been applied to all components.
- Run only services required to meet desired functionality (disable unused services).
- Identify and enable required TCP/UDP ports and disable other TCP/UDP ports when applicable.
- Log all security related events including unauthorized attempts to access privileged services.
- For data encryption. Symmetric cryptosystem key lengths must be at least 128 bits. Asymmetric crypto-system keys must be of a length that yields equivalent strength.

B. Security Design & Review

- Selected Contractor shall submit a network diagram for approval by LAWA IT Security.
- Selected Contractor shall submit an application flow diagram for approval by LAWA IT Security.
- Selected Contractor shall be required to show that the network and/or application flow design conforms to security best practices.

C. Documentation

Selected Contractor shall provide a security plan that include, but is not limited to:

- An overview of the information system security posture.
- Technical details regarding information system implementation strategy, documentation or guidelines that vendor follows to implement and deliver the information system.
- Technical details regarding security strategy - patches applied, operating system hardening steps, services enabled/disabled, TCP/UDP ports opened/closed, authentication requirements, etc.
- Any deviations from the security best practices shall be documented by the Selected Contractor and must be approved by LAWA IT Security.

D. Security Assessment

Selected Contractor shall conduct a security risk assessment (ISO/IEC 27001 and 27005) prior to deployment to ensure appropriate security controls have been designed and implemented. LAWA IT Security, or a third party representing LAWA, shall conduct a security risk assessment prior to final user acceptance, and semi-annually.

E. Security Issue(s) Remediation

Provision for remediation of security issues as requested by LAWA:

- The Selected Contractor must immediately remediate vulnerabilities and high-priority security issues identified during a security review or assessment.
- The Selected Contractor shall be responsible to remediate high and medium risk level issues within a reasonable timeframe. If the remediation affects the functionality of the system, LAWA IT Security may grant an exception depending on the risk level or use other external security methods to mitigate the risk.

Additional security assessment may be performed after remediation for verification purposes at the discretion of LAWA IT Security.

F. Cloud Security – Software as a Service (SaaS)

SaaS provides LAWA client the capability to use the provider's applications running on a cloud infrastructure. LAWA does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage with the possible exception of limited user-specific application configuration settings.

Requirements for Cloud Provider:

- Must be SSAE 16 SOC1/SOC2 or ISO 27001/27002 compliant on all hosting facilities; and provide compliance audit report semi-annually.
- Ability to provide regulations & compliance control solution.
- Ability to provide identity management solution (such as active directory Integration, multi-factor authentication, cloud access security broker (CASB), and single sign-on).
- Ability to provide data access control solution.
- Ability to detect and block unauthorized/malicious traffic on the network (such as botnet/malware, SQL injection, cross-site scripting, denial-of-service, etc.)
- Ability to provide data protection/encryption/segregation solution.
- Ability to provide anti-virus and patch management solution.
- Ability to provide key management solution
- Ability to provide business continuity and disaster recovery solution (such as alternate site, backup/recovery procedure, recovery point objective, recovery time objective).
- Ability to provide security incident response solution.
- Ability to response and provide immediate notification to LAWA on all security breaches, system failure, and network outages.
- Ability to provide LIVE application/data security feeds to LAWA.
- Ability to provide service level agreements on reliability, availability, performance, customer support, and penalties.
- Ability to provide data retrieve/removal solution when contract terminates.

G. Vendor Hosted Systems Service Provider

Vendor Hosted system services are those services where LAWA does not manage or control daily operations, application or system services, infrastructure, network, servers, operating systems, or storage.

Requirements for Vendor Hosted system services:

- Must follow industry best practice security standards when providing Industrial Control Systems.
- Must ensure PCI DSS compliance when dealing with payment cards and PII.
- Ability to provide regulations & compliance control solution.
- Ability to provide identity management solution (such as active directory Integration, Multi-Factor Authentication, single sign-on).
- Ability to provide data access control solution.
- Ability to detect and block unauthorized/malicious traffic on the network (such as botnet/malware, SQL injection, cross-site scripting, denial-of-service, etc.)
- Ability to provide data protection/encryption/segregation solution.
- Ability to provide anti-virus and patch management solution.
- Ability to provide key management solution
- Ability to provide business continuity and disaster recovery solution (such as alternate site, backup/recovery procedure, recovery point objective, recovery time objective).
- Ability to provide security incident response solution.
- Ability to response and provide immediate notification to LAWA on all security breaches, system failure, and network outages.
- Ability to provide LIVE application/data security feeds to LAWA.
- Ability to provide service level agreements on reliability, availability, performance, customer support, and penalties.
- Ability to provide data retrieve/removal solution when contract terminates.