East Bay Municipal Utility District

DAM System and EBMUD Archive Scanning and Consolidation

EXHIBIT A

Preliminary Security Information Gathering (PSIG)

Preliminary Security Information Gathering (PSIG)

As a component of the supplemental RFP process, EBMUD will be performing a qualifying evaluation of each of the RFP respondents Information Protection program. Please respond to the following questions, keeping your responses as brief as possible, please limit your responses to no more than five (5) pages in total. If your organization is selected you will have the opportunity to provide more in-depth responses during the formal security review.

A. Risk Management

Objective: Organizations should create and maintain a continuous process for IT and Infrastructure risk management to identify, quantify, and prioritize risks against defined risk acceptance levels and objectives relevant to the organization.

1. Describe your organization's IT Risk Governance
2. Describe your organization's IT Risk Life Cycle

B. Information Security Policy

Objective: Organizations should provide management direction and support for information security in accordance with business requirements and relevant laws and regulations. They should set a clear policy direction in line with business objectives and demonstrate support for, and commitment to, information security through the issue, acceptance and maintenance of an information security policy across the organization.

1. Describe your organization's Information Security Policy
2. Describe how the policy or policy set is reviewed and maintained, include the frequency of review

C. Information Security Organization

Objective: Organizations should establish a management framework to control and manage the information security organization. This should include the protection of organizational information through the use of employee confidentiality agreements and the addition of clauses in dependent service provider contracts or agreements.

1. Describe the size and structure of your Information Security department.
2. Does your organization rely on dependant service providers? If so, how is their security vetted by your organization?

D. Physical and Environmental Security

Objective: Organizations should take appropriate steps to prevent unauthorized physical access, as well as accidental and intentional damage to the organizations' physical premises, systems and information. Organizations should also take appropriate steps to protect against environmental and systems malfunctions or failures.

1. Describe the physical controls in place at your data center(s)
2. Describe the environmental controls in your data center(s)

Preliminary Security Information Gathering

E. Operational Security

Objective: Organizations should maintain documented operating procedures and technological controls to ensure the effective management, operation, integrity and security of their information systems and data.

1. Describe the operational controls in place
2. How does your organization log and monitor system and network activity?
3. Describe your intrusion detection methodology
4. Describe your organization's data backup and restoration process
5. Describe your organization's change control process

F. Access Control

Objective: Organizations should ensure sufficient control over access to information, including controlled access to target data and information processing systems and facilities. These controls should be based on security and business requirements, and should follow both industry best practices and internal policies.

1. Describe your organization's access control policy
2. How does your organization handle privilege delegation and separation of duties?
3. How does your organization handle inactive accounts and access revocation?

G. Software Development and Maintenance

Objective: Organizations should utilize a comprehensive application security program to help ensure that external high-risk applications are consistent with industry security requirements. This should include full application compliance testing and software development reviews.

1. Describe your Software Development Lifecycle
2. Describe your application vulnerability assessment methodology
3. Describe your application and system patching strategy.
4. What is the frequency of application and system security review?

H. Incident management

Organizations' incident response programs should include formal event reporting and escalation procedures that should be clearly communicated throughout the organizations, and should include the active participation of incident response members with clearly defined roles and responsibilities.

1. Describe your incident management program

I. Business Continuity

Objective: Organizations should 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 should 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.

1. Describe your Organization's Business Continuity program
2. Has your Organization performed a recent Business Impact Analysis?
3. Does your organization have a current Threat Assessment?
4. How often is your business continuity plan tested?

Preliminary Security Information Gathering

J. Regulatory Compliance

Objective: Organizations should ensure compliance of information systems with the organizational security policies and standards to include checking systems regularly against compliance with security implementation standards and regulatory requirements.

1. How does your organization ensure compliance with internal policies and standards?
2. How do you ensure compliance with Federal, State, and local laws?

K. Privacy

Objective: Organizations should establish a management framework to control and manage their privacy program. This should include the overall management of the privacy program within the organization and with all third parties that have access to target privacy data. The privacy program should include: individuals responsible for the creation, oversight and maintenance of the program; all third parties meeting their commitments under the organization's business requirements, privacy applicable law, policy and industry best practices; and the protection and privacy of target privacy data through its life cycle of collection, storage, usage, sharing, transferring, securing, retention and destruction.

1. Describe your organization's Privacy program