Reference Solicitation URL: https://sam.gov/opp/7e227d7bd2c84918b0147211c8aeac30/view

Overview Synopsis:

The document provided pertains to an opportunity for an Immersive Learning Management System (ILMS) known as SIMPLE ILMS, with the solicitation number 36C10B23Q0375. The opportunity is issued by the Department of Veterans Affairs (VA) and is seeking contractors or subcontractors to fulfill the information security requirements for working with VA systems and data. The document outlines various sections related to information custodial language, system design and development, system hosting and operation, security incident investigation, liquidated damages for data breach, security controls compliance testing, and training.

Section-by-Section Synopsis:

General Information:
This section provides basic details about the opportunity, including the contracting office's zip code, solicitation number, and response date/time/zone.

Information Security Checklist:
This section includes a checklist with questions related to information security. The subsequent sections in the document correspond to the answers provided in this checklist.

VA Information Custodial Language:
This section emphasizes the proper use and protection of information provided by VA. It highlights the need to separate VA information from other data, return or destroy VA information as per VA's requirements, comply with information confidentiality and security laws, and seek approval for any uses or disclosures of VA information.

Information System Design and Development:
This section focuses on the requirements for designing and developing information systems for VA. It covers compliance with VA directives, security configurations, software installation guidelines, user privilege management, security controls design and implementation, Privacy Act compliance, and adherence to NIST guidelines.

Information System Hosting, Operation, Maintenance, or Use:
This section addresses the hosting, operation, maintenance, or use of VA information systems. It includes requirements for compliance with HIPAA, Privacy Act, FISMA, NIST, and VA directives, security control assessments, outsourcing agreements, self-assessments, media sanitization, and equipment usage guidelines.

Security Incident Investigation:
This section outlines the procedures for reporting security incidents, cooperating with investigations, and notifying relevant parties, including the COR, ISO, Privacy Officer, and law enforcement authorities. It highlights the need for prompt action in case of security incidents or criminal activities.

Liquidated Damages for Data Breach:

This section explains that contractors may be liable for liquidated damages in the event of a data breach involving sensitive personal information (SPI). The contractor must provide notice of the breach to VA, and an independent risk analysis will determine the level of risk associated with the breach. Liquidated damages may be required to cover credit protection services for affected individuals.

Security Controls Compliance Testing:
This section highlights VA's right to evaluate security controls and privacy practices implemented by the contractor. Contractors must cooperate with security control assessments conducted by VA, including unannounced assessments by the Office of Inspector General.

Training:
This section outlines the training requirements for contractor and subcontractor employees who need access to VA information and systems. It includes signing the VA Information Security Rules of Behavior, completing privacy and information security awareness training, and additional cyber security or privacy training as determined by VA.

Minimum Criteria for Responsiveness:

To be responsive to this opportunity, a company must:

- Have experience and expertise in developing and maintaining immersive learning management systems.
- Demonstrate a clear understanding of VA's information custodial language, information system design and development requirements, information system hosting and operation guidelines, security incident investigation procedures, liquidated damages for data breach, security controls compliance testing, and training obligations.
- Provide evidence of compliance with applicable federal and VA information confidentiality and security laws, regulations, and policies.
- Have the capability to implement and manage security controls, conduct security control assessments, and participate in VA's security control and privacy practice evaluations.
- Possess the necessary infrastructure, resources, and technical expertise to host, operate, maintain, or use VA information systems while adhering to relevant standards and guidelines.
- Demonstrate a commitment to privacy and information security, including personnel training and awareness programs.
- Be willing to cooperate with VA's security assessments, incident investigations, and reporting procedures.