2131 PALOMAR AIRPORT RD., STE. 239
CARLSBAD, CA 92011
800.240.3280
WWW.911EDA.COM

Cloud Service Compliance Guide for 911EDA Inc.

911EDA, Carlsbad CA 92011

Introduction

As 911EDA Inc. embraces cloud technologies to enhance operational efficiency and innovation, it is imperative to ensure the security and integrity of defense-related information stored and processed in cloud environments. This guide outlines our approach to cloud service compliance, specifically adhering to the Defense Federal Acquisition Regulation Supplement (DFARS) requirements and the Federal Risk and Authorization Management Program (FedRAMP) standards.

Purpose

This guide serves to inform our employees, contractors, and partners about the criteria and processes 911EDA Inc. employs to select and manage cloud service providers (CSPs). Our objective is to ensure that all cloud services used in defense contracts comply with DFARS Clause 252.204-7012 and meet or exceed the FedRAMP Moderate baseline security controls.

Scope

The scope of this guide encompasses all cloud services and platforms utilized by 911EDA Inc. for storing, processing, or transmitting Controlled Unclassified Information (CUI) or any other defense-related data. It applies to all decisions related to the selection, implementation, and ongoing management of CSPs.

Cloud Service Provider Vetting Process

1. **FedRAMP Compliance**: Initially, we ensure that the CSP holds a current FedRAMP Moderate Authorization. This certification demonstrates that the CSP has implemented a robust set of security controls sufficient to protect federal government data.
2. **DFARS Clause 252.204-7012 Compliance**:
    - We verify that the CSP is capable of adhering to the security requirements specified in DFARS Clause 252.204-7012, which includes safeguarding covered defense information and reporting cyber incidents.
    - Specifically, we assess the CSP's ability to provide adequate security to protect covered defense information and their process for reporting cyber incidents that could affect the covered defense information or the ability to perform requirements designated as operationally critical support.
3. **Data Sovereignty and Localization**: Given the sensitivity of defense contracts, we ensure that data stored in the cloud is hosted in secure data centers located within the United States, complying with data sovereignty requirements.
4. **End-to-End Data Encryption**: We require that the CSP supports end-to-end encryption for data at rest and in transit, using cryptographic standards that comply with federal guidelines.
5. **Continuous Monitoring and Incident Response**: The CSP must have a continuous monitoring program that aligns with federal standards and an effective incident response plan that meets the rapid reporting requirements of DFARS.

Ongoing Compliance and Management

- **Regular Audits and Assessments**: Conduct periodic security assessments of the cloud services to ensure ongoing compliance with FedRAMP and DFARS requirements.
- **Contractual Obligations**: Include specific security and compliance requirements in contracts with CSPs to ensure they understand and commit to meeting these obligations.
- **Employee and Contractor Training**: Provide training on the use of cloud services, emphasizing the importance of compliance with federal regulations and the protection of CUI.

Conclusion

Leveraging cloud services offers numerous benefits to 911EDA Inc., from enhanced flexibility and scalability to improved efficiency. However, it is crucial that these services do not compromise the security of defense-related information. Through diligent vetting, continuous management, and adherence to federal compliance standards, we ensure that our use of cloud services supports our commitment to protecting national security interests.

This Cloud Service Compliance Guide underscores our dedication to maintaining the highest standards of compliance and security in all aspects of our operations, particularly in the utilization of cloud technologies.