**Proposal to the
Office of Systems Integration
(OSI)**

**Request for Information (RFI)
#75001**

**For
Agile Development Pre-Qualified
(ADPQ) Vendor Pool**

Continuous Monitoring

June 4, 2016

SafeKids

X FUSION
TECHNOLOGIES

Strategy! Innovation! Transformation!

Revision History

Version	Date	Description of Updates	Author
DRAFT	05/30/2016	DRAFT Version created	xFusion
1.0	06/04/2016	Updated with review comments	xFusion

Table of Contents

List of Tables

NO TABLE OF FIGURES ENTRIES FOUND.

LIST OF FIGURES

No TABLE OF FIGURES ENTRIES FOUND.

1. Introduction

xFusion's development, maintenance, and operations include continually monitoring preventive and detective controls using industry standard tools. For our products, we use the Amazon Web Services (AWS) environment for production, and heavily use the tools that AWS provides. Additionally, we follow the National Institute of Standards and Technology (NIST) Publication 800-37 recommended controls, which include:

- Configuration Management
- Security Impact Analysis on Changes
- Assessment of Security Controls
- Security Status Reporting
- Active Management of Security Risks

2. Continuous Monitoring

xFusion uses the AWSConfig and AWSCloudtrail provided by AWS for continuous monitoring of the SafeKids application. This monitoring includes:

- Management of the vulnerability, configuration, and IT assets.
- Real time visibility into the system security posture through regular monitoring
- Security metrics through AWSConfig Reporting.
- Threat intelligence through alerts and visibility using AWSCloudtrail Reporting
- Intrusion Detection

The AWS tools provide monitoring and prevention of inappropriate or unauthorized changes to the security baseline.

3. Initial Configuration

The initial baseline for the SafeKids application was created using the AWSEBS and other support tools in the EC2 environment, which provided recommendations for our product development team to implement based on best practice results. Our team also did an inventory analysis to verify:

- Running instances
- Storage used
- Identity and Access Management (IAM) groups and users
- Hosted zones and health checks