

Task 3.3 Incident Response Program

Task Overview

FSA and its partners operate numerous systems at several locations using many platforms. While constructed securely, system incidents will inevitable occur. Understanding this inevitable situation, FSA needs to develop an incident response program to identify, mitigate and recover from malicious and non-malicious cyber attacks. The program will include plans for notifying affected parties, escalating responses, and coordinating with the Departmental incident response program.

Task Details

The objectives and milestones identified for this task are as follows:

Objective(s):

- Coordinate FSA efforts and methods to conform with the OCIO incident response program
- Review policy and develop procedures for notifying cyber incident affected parties
- Review policy and develop procedures for escalating incident responses and for reporting incidents to the Department level.

Milestone(s):

- Review (read) Department Level Incident Response Program (and FSA program as it currently exists)
- Meet with EDCIRC personnel to determine what FSA can do to comply with OCIO's incident reporting requirements.
- Meet with FSA Incident Response personnel
- Questions and Network Map (physical and system administrator views)
- Document incident response procedures based on acquired information
- Develop training session and awareness materials

Task Status

At this time all the objectives and milestones for this task have been completed.

We will continue to work with FSA and EDCIRC as the incident response program is implemented. We will assist in the compilation of the FSA Incident Response Contact List. We will encourage attendance to the Department's IR training courses. We will also continue to work with the Department in publishing and providing quick guide, desk materials for incident response. We anticipate further meetings with contractors and FSA personnel to address specific incident response questions and issues.