

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

The objectives and milestones for this task have all been completed. We have provided an updated FSA Incident Response Implementation Guide, which now includes "incident prevention" and patch management. We have participated in an update meeting with the Department in regards to EDCIRC status. This meeting highlighted FSA's commitment to move from simple security incident reporting to also follow guidelines for routine reporting of suspicious activity and to find ways to take on more of the incident response capabilities. We will continue to work with FSA and EDCIRC to unfold the entire incident response program.