

Incident Response at FSA: Implementation Steps, Requirements and Issues

For a solid IR program FSA needs to take several steps. The first step is for all FSA to start by only changing one major aspect – reporting.

First Step requirements are:

- Security tracking logs, and event logs should be activated on all systems
- All logs are to be reviewed at least once daily trying to find events that are security incidents.
- All logs are to be kept for one year.
- Fill out either a contractor report form (if it already exists) or the Department provided SER (Security Event Report) and submitting it to the SSO when an Incident is found.
- Following instructions on preservation of evidence.
- Provide for alternate system capability (Continuity of Service)
- Be ready to work with and follow EDCIRC/EDS instructions.

In this first step the requirement for monitoring and review of systems will remain the same. System logs are to be reviewed daily and per the FSA security policy are to be kept for one year. All of this is established and will not change. Personnel and Contractors have previously been required to report security incidents and secure potential evidence. However, a formalized contact list/process, reporting time frames, and preservation of evidence procedures has not previously been present. It also recognizes that FSA is using the IR analytical and forensic services provided by EDCIRC and an OCIO contractor, and that contractors need to be ready to work with these organizations in providing information, data and possibly the compromised hardware to resolve a security incident. This first step simply formalizes and standardizes these items – there should be nothing in them that creates more work, or that creates the need for anything more than currently exists. It is a matter of just knowing what the next proper step is.

The first step should not be complicated and *FSA has developed a document (FSA Incident Response Implementation Guide that will provide the requisite knowledge (i.e. a contact list, a reporting tree, acceptable reporting time frames, an incident response flow chart, and information on preserving evidence.)* The possible areas that might require modifications could be:

- 1) **Daily** review of logs, as this may not be a part of current contracts even though this is a well established industry best practice.
- 2) Keeping a copy of the daily logs for **one year**, this also may not be a part of current contracts as it became official with the publication of FSA's IT Security Policy and one year exceeds commercial expectations.
- 3) Continuity of Support (COS)/Disaster Recovery (DR) is a fairly new officially established FSA policy, however the same concept may be covered by established Service Level Agreements (SLAs).

If these do become issues it may be best to let the contractors continue current practices and make no requirement other than the reporting and preservation of evidence and working with EDCIRC. Then, all modification could be addressed at the Second Step.

The Second Step for FSA will be to implement suspicious activity reporting.

Second Step Requirements are:

- Formal weekly report on Category B Suspicious Activities
- Formal monthly report on Category A Suspicious Activities
- Be ready to work with and follow EDCIRC/EDS instructions.

Suspicious Activity reporting requirements provided by the Department of Education divide suspicious activity into two groups. Depending on the group classification the activities will be reported either weekly and monthly. Such reporting, while not a large requirement, is obviously a change to current practices and contracts. It is a definitely a new requirement and contract modifications will need to be made.

The second step is not complicated either. *The FSA Incident Response Implementation Guide that has been developed also covers the requisite knowledge and explanation for this area as well.*

Once the second step is implemented FSA will have a complete, basic, Incident Response program in place.

However, FSA is not yet finished. The Department of Education is coming out with an “Incident Handling Guide”. This document will be considered the primary source for Incident Response. The Guide will contain precise procedures and standards. The procedures and standards in that document need either to be followed or have an EDCIRC approved substitute. *The potential for contract modifications in order to comply with the Guide is significant. Not that it is difficult to implement but rather it may mean many small changes to the way things are currently done or handled and might mean an increase from the basic services contractors currently supply.* Plus there may be one-time start-up costs associated with getting things in place. FSA will need to review each contract to see what services were contractually agreed to and what needs to be modified.

FSA will initially use the EDCIRC IR services, which are already paid for by the Department (whether a PO will have to “pay back” the Department remains unanswered). FSA needs to investigate having the contractors provide Incident Response capabilities as part of their contract and/or to set up an FSA CIRC that would centralize incident response and its resolution in FSA (all of course following the Departments guidelines – and being approved by the Department). Both options are likely to be substantially more expensive and a business model and need would have to be expressed to justify such an expense over the current model.