

OIG GISRA Report Review

Some general comments:

As we discussed, I don't think there are many areas that FSA can complain about too loudly, although that has a lot to do with the lack of specifics the IG gave when talking about PO discrepancies (I'll expand on that in a bit). Most of the findings were Department-focused, with a lot of generalized speech that can't be easily rebutted. It will be interesting to see the Department's response, although I'm sure they won't focus on what may have been wrong with the IG's findings, but rather on what a wonderful job Ed's done and how they will continue leading the way in federal IT security.

I figure the VDC needs to respond to the technical findings, so I didn't examine those too closely. One item I am curious about is why IDS is set to exclude internal traffic. Was this a risk-based decision because of data speed requirements, resource capabilities, etc.? At the very least, the decision should probably be looked at again. If it still makes sense, then so be it.

As to the lack of specifics regarding discrepancies... For the management and operational findings, the IG report should (preferably) provide an appendix listing the systems examined and the discrepancies noted. At the very least, they should list the systems that were reviewed. Instead, they state that "## of 16 Department mission-critical systems that we reviewed" had a problem with whichever issue they were looking at in that section. From a PO perspective, it makes it difficult to implement changes based on the report. Not only is it not possible to determine which systems were negligent, it's not even possible to determine which systems were actually examined.

Some specifics comments:

p.21 discusses the IG's suggestion that the Secretary should endorse the Department's IT Security Policy. As we discussed, until their security policy is ready and useable, that would probably be a bad move - now you've got the entire department worried that they aren't capable of following an unreadable document.

p.28 - SDLC - Even though the IG is pointing out that the Department (vs. specific systems) does not have a life cycle plan, it may still be a good move to remind them that FSA has one in place.