

We really appreciate the in-depth analysis and review of FSA's policy document, and will implement many of the suggestions provided. It was great to receive such specific editing; it will help us achieve our goal of providing FSA clear, concise, and useful security policy guidance. Below we have included our responses to your suggestions.

Most of my Specific Comments. I didn't have time to read in depth or wordsmith to be kind or politically correct, but the comments are direct and to the point.

Page 3

1.2 Scope. Line 7 typo, two periods after "facility" Agreed

Last sentence does not read well. While FSA policy addresses FSA organization, the fact FSA policy is based on Dept. policy and minimum standards does not put the ED resources within FSA outside the scope of the FSA document. Consider dropping this sentence. Will rewrite as "External IT resources" are outside of the scope of the document. The Title of the Department document is also not correct. (**Information Technology Security Policy**) Agreed

1.3 FSA Security Fundamentals, Bullet 3. This section is not clear. The first bullet should stop after the word 'process...' Agreed and the second bullet needs to include security also. Disagree – that bullet talks about separation of environments; the previous bullet covered duties (including security). Bullet 5 is not recommended as a policy statement because it could weaken the risk management of system security as stated. Whether a system is secure or not should not be 'judged' on how customer's 'view' the protection provided. While this can play a role, it does not belong in a policy statement or openly mentioned in an overall security policy and strategy. Agreed – that bullet describes more the purpose of security – to provide systems worthy of trust. It's information will be moved to the end of Section 1.1.

1.5 Exceptions. Not clear on what exceptions will require higher-level approval. Who decides if higher level approval is needed, the CSO? What are the criteria and to what guidance shall the reader go to and get that guidance? Will rewrite to include determining approval level of exceptions and possibility of Department-level waivers.

1.6 Applicability. Does this apply to end users at GA and schools level? What defines 3rd parties?? Changed "third parties" to "parties" for clarity. Essentially, the first paragraph discusses personnel under FSA control. End users as GA and schools are what the second paragraph discusses.

Paragraph 2, what is the difference between a partner and a 3rd party? Various program participation agreements and contracts is a very broad and vague statement to make when discussing applicability. Consider either defining these items or remove this sentence. Will rewrite for clarity. Final sentence, how can you enforce policy on a terminated employee or contractor support person? There is nothing legally binding that permits this. If there is, specifically state what it is that makes this statement true. Agreed; will remove.

1.8, the title for 800-18 is incorrect Will correct, also several key laws are not referenced. Computer Security Act, Govt. Paperwork Elimination Act, PDD-63, Clinger-Cohen Act.... to name a few. We only referenced the documents directly reviewed to create the policy document. As Footnote 2 mentions, requirements from many federal laws were included in NIST 800-26, so we only included the NIST document.

Page 6. 1.10 Second sentence, how do you document this action for auditability? To what guidance do you point to so this can be done properly? Procedure, not policy. Having the SSO appointed by the system manager is a conflict of interest as is making the system manager the overall security decision maker for the system. The SSO roles are basically reduced to being a clerk for the system and this is not advised. As written this places too much security power in the System managers hands and violates separation of duties related to security functions as A-130 requires. It is recommended that both the system manager and SSO oversee daily security duties, but the functional manager calls the shots and appoints the SSO. Will review and update per business operations.

The second paragraph contradicts the first by placing security policy responsibility in the CIO, but the COO is held responsible. There is a disconnect in delegation of authority that must be addressed here. Disagree. The CIO may be responsible for creating the policies, guidelines, etc. but that does not take away from the COO's responsibility of the agency's overall operation. The COO is responsible for how people operate the systems, ergo has ultimate responsibility for security.

Page 7, 2.0, Paragraph 2 provides errant policy. System managers should not be making the risk based decisions for a system, the system owner does. True, however the system managers are responsible for "implementing" the decisions, as it states in the document. We will change "cost effective policies" to "cost effective security measures" for clarity. In addition, you introduce two divergent philosophies, risk based, and business type decisions. Either one or the other takes precedence. One is devoid of risk-based processes and is purely bottom line money driven decision-making. Disagree – one must balance risk-based and business-type decisions in order to provide a service that is cost effective, yet not completely vulnerable. OMB A-130 proscribes this method. This paragraph also fails to acknowledge that legislation does play a role regarding to what minimum level security decisions can go. Agreed – will include.

2.1 Risk Management, This places too much security decision-making power at the system manger level and takes the system owner out of the process. Will change "Channel Leadership" to "System Owner" for clarity. This is a conflict of interest. It is the Functional Manager, or system owner who drives the decision making process for the IT systems that support their function, not the other way around as this section has it. Bullet 3 is not a system manger function; it is the business manager's function to oversee/conduct business impact assessments/analysis. The supporting IT system manager is a key part of the process, but does not drive it. Disagree – the BIA is part of the risk assessment process, which the SM drives. This also introduces the possibility of

a conflict of interest, or at a minimum a serious possibility of biased results. This is why an independent assessor must complete the risk assessments.

Page 8, Bullet 4. Risk mitigation recommendations should come from the SSO AND system manager to the system owner. Will clarify by changing “program official” to “System Owner”

Last sentence in 2.1 relegates the SSO to a clerical duty in risk management for a system when in fact the SSO should have a lead role. Disagree – this may be their primary role during risk management, but doesn’t mean that this is their sole duty.

2.2 paragraph 2, "If security incidents or significant weaknesses are found...", makes no sense. Security weaknesses are all you have to mention. It also does not mention whether that action must be immediate or if another evaluation process (risk management) takes over. Will remove “security incidents”

Paragraph 3 makes no mention of to whom these assessments are reported. The findings are not reported directly from FSA to OMB, they must go to ED proper, the CIO's office specifically. **The final sentence is not appropriate and contradicts ED policy. System managers cannot accept risk; only an authorized DAA can do this.** Good point – this document was completed before the Department’s C&A guidance was completed. Will change from SM to DAA.

2.3 this section does not say who approves a system security plan. Will rewrite – SSPs do not need to be approved, but they do need to be in proper 800-18 to pass certification. Will rewrite.

2.4 Bullet 1, define conditional? Under system rules of behavior, conditional rules can introduce vulnerability and increase risk. Disagree – conditional as in dependant on certain conditions. (For example) If someone is working from home (condition), they must perform these additional actions. Rules of behavior are never to be ‘optional’ either you have them, or you don't. Agreed – will remove.

Bullet 2. Simplify this bullet. Will reword.

Page 10, 2.7 Privacy act training is not addressed as the heading suggests. Disagree. Not talking about Privacy “Act” training. Additionally, privacy training is discussed in the first paragraph, last line.

2.8, Bullet 5 should read, the Department's right to audit. This includes the Inspector General's Office Agreed – will change.

Bullet 7, needs to include the COR and CO. Agreed – will check with contracting to determine if both need to be notified or just the COR.

Page 11, 3.1 the last bullet talks about compliance with a process, but this section fails to mention what that process is, or where it is documented. The process is the entire set of personnel security controls, and further information is provided in section 3.1.8. More detailed documentation would be procedure, not policy.

3.1.1, Paragraph 2, it mentions "the SSO, or designee. There is no mention of designee in the roles and responsibility section on this. Who appoints the designee and on what authority? Will remove "designee"

Page 12 3.1.2. The system manager is identified as the official who designates risk levels for positions, but there is no reference as to a guide or process on how to accomplish this and who approves those levels as acceptable or accurate. The SSO should do that and the system OWNER approves them. Will change so that supervisors create job descriptions, and SSOs designate sensitivity levels.

3.1.4 references handbook 11, but this document is not in the list of referenced documents at the beginning of this policy/ Will add to the references.  
Renewal of screenings every 5 years for all levels is more stringent than ED's overall policy, and the Federal government's for that matter. There may be cost factors involved that would prohibit this being implemented for ALL FSA fed and contractor staff. You need to talk with the ED Personnel Sec officer on this first. Agreed – will change to "for high-risk positions"

The last sentence does not indicate where these procedures can be obtained. Procedure, not policy.

**3.1.5 This contradicts ED policy.** System managers are not the sole decision maker for external connections to a system. Interconnection requires a full C&A reassessment, MOU[s must be written and approved by the system owner and the DAA. This is all part of complying with FSA security standards.

It mentions sensitive data cannot be left unattended unless safeguarded properly, but in accordance with what standards? This policy has not even addressed who authorizes an individual to load sensitive information onto portable computers. Procedure, not policy.

3.1.6 fails to cover documents that are by-products of system output. Also it fails to identify which FSA policies apply here. The policy does cover the information on the documents, and therefore the documents themselves.

3.1.7. This section fails to address security duties, and does not go far enough in separation of duties over all. Good start but needs to be complete. Will add security within list of expertise.

3.1.8, To whom does the System manager report their compliance results? Procedure, not policy.

3.2 Define adequate? In accordance with whose policy and standards? Who decides what controls are adequate? This is only the introductory paragraph. Details are in the following subsections. Will remove "adequate".

3.2.1 This does not address contractors in first paragraph. Agreed – will add. It also fails to address offices where hard copy or soft copy output from systems are stored.

Agreed – will add. Paragraph 3 mentions changing of access codes (if applicable), but codes for what? cypher locks? key pads, what?? Are these things required? Under what conditions? Where are the criteria for determining if such devices are necessary?

Procedure, not policy.

Page 14, the last sentence in first paragraph needs to be restated. It is requiring any FSA staff person to investigate possible incidents, which is an unacceptable policy. Only security staff appropriately trained should do this activity. Agreed – will rewrite. But procedures for reporting incidents are needed and there is no reference here that points to guidance or FSA staff on how to do that. See Section 3.8 (Incidence Response) The last sentence in the second paragraph is a technical control, not a physical security control. Partially agreed; this is where NIST 800-18 discusses protection of mobile devices, and the reason why you would encrypt is in case your device was physically stolen.

3.3 The last sentence mentions an input/output incident, but this definition is not found anywhere. Will change to “incident involving the input or output of data”.

Page 15, 3.4 **The second paragraph is wrong.** It places a key decision in a system manager's hands when it belongs in the functional manager's (system owner's) hands. Agreed – will change. Last paragraph is way beyond an SSO's responsibilities. SSOs have the responsibility of driving the task towards completion, but will most likely have a contractor actually complete the task. An SSO alone cannot complete a contingency plan, nor can they authorize a system for processing. Which is what the first sentence implies. Agreed – will change. Contingency plans incorporate far more than risk assessment results. True, but that is not the purpose of the second-to-last sentence. The contingency plan should be completed covering all aspects of the system; when updating the plan, they should pay particular attention to identified system weaknesses as that is most likely where an incident may occur.

3.4.1 Page 16, The last sentence at the top is the first reference to the DAA...Who is that in the roles and responsibilities of this program? Waiting for Departmental guidance... Also, the system owner is not mentioned in this process. Agreed – will add. Again, the system manager is given too much security decision making power, when it should rest with the system owner and DAA.

3.5.1 The first sentence should state that virus detection and eradication software is to be installed on all devices, not systems. A system can be made up of tens of devices. If only one has the software the system owner can say they complied, which is hardly the intent of the policy. Disagree – not all devices need anti-virus software (firewalls? hubs? etc.). Will reword to clarify – “systems and their applicable devices”.

NOTE: Non-repudiation is not mentioned in this area. Any reason why it is left out?? See section 3.5.4.

3.5.6 This section fails to include the SSO, who is a key position in this process. Agreed, will change. Paragraph one is devoid of policy regarding what happens when an

intrusion is detected, to who is it reported, who is responsible for reaction and correction? See Section 3.8 (Incidence Response) It also only mentions log review, implying that IDS will not be a real time monitoring function. Last sentence puts IDS report review on the system manager AFTER and incident. Real-time monitoring (if applicable) would be contracted. Paragraph 2 intimates to incidents but falls far short on proper policy surrounding incident handling. See Section 3.8 (Incidence Response)

3.5.7 System managers overseeing penetration testing is a direct conflict of interest if the policy intent is to require 'independent' testing. Purpose of independent assessors. This section does not state to whom the results are reported to. Procedure, not policy.

3.6 Sentence 1 is describing a system security plan, so just say it that way. Not necessarily – describes the list of documents in this section. Who is responsible for making sure the SM maintains the documentation? Part of policy compliance – will occur during self-assessments, IG inspections, audits, etc..

Page 19, first bullet, top, The SSO must be a member of the group, not just attend the meetings, otherwise there is no point for them to be there. Agreed – will reword.

3.7.1.1, Bullet 4, Live data is NOT to be used for testing in any instance unless the DAA signs off on it. Will reword.

Bullet 7 This is not very clear what this is trying to cover. CM requirements for emergency repair.

Last bullet, include the word TIMELY at the beginning. Agreed – will add.

3.7.2.1 This policy is contradictory. It says to reset defaults to a restrictive setting in all instances, but then states "where necessary". Must change all settings to “a restrictive setting. Where necessary” (most sensitive areas/based on threats), “use the most sensitive” No contradiction. This is not entirely the system managers' decision alone. The SSO and system owner should be the ones to do this. Agreed, will make changes.

Remote system maintenance can only be approved by the DAA during C&A process. Will add. Last paragraph first sentence conflicts with ED policy. Services that are not necessary are to be disabled and removed from IT resources, not "when possible". The idea was regarding a service that was prohibitively expensive to remove – if the DAA makes a risk-based decision, it should be allowed to remain. As soon as possible, the system should be upgraded to remove the unnecessary service. Will rewrite.

3.7.2.2 **Second para graph contradicts ED policy.** Installation of personal software on ED assets is prohibited unless approved in writing from ED CIO. Will add approval requirement.

3.7.2.3 Software developed in house becomes FED property; also software developed while under a contract becomes FED property in most cases. Simplify this sentence. Will change.

3.8 This section is weak and does not indicate any policy regarding incident handling. Who is responsible for reporting incidents? Reacting to incidents? Where are the procedures located referenced in this policy???

Procedure, not policy.

3.8.1 No reference to ED level connection to ED security program is mentioned.

Will add.

3.8.2 SSO's are totally left out of this process. Agreed – will change. This is a flaw in the policy and the program. No guidance information is noted nor its location so users know where to go to find out how to do this. Procedure, not policy.

3.8.3 Improving response technique or process is not mentioned. Agreed – will add. Where is the guidance for the system managers on how to respond to incidents? Also the system managers should not be directing incident response in a vacuum, which is also what these few policy statements imply. I doubt it is FSAs intent to have a collage of incident handling and response procedures that vary from system to system. Procedure, not policy.

Page 22

4.1 The supervisor is totally out of the loop on authorizing access to systems. Agreed – will add. Also I&A is used to ensure accountability for actions on a system. This needs to be added. Agreed – will add. This policy also does not identify who can authorize a user to by-pass controls, nor does it address the impact on the user's security screening levels. So as written, a low risk user could obtain authorization to by-pass controls simply by stating a "need" to the system manager. Procedure, not policy.

3rd paragraph talks about limiting attempts to access but does not provide a maximum standard. It only says they need to document how many. Procedure, not policy. It also does not require disabling the account. Procedure, not policy. Also, part of "actions taken" by the SSO.

4th paragraph the first sentence doesn't make any sense. It is not clear what this policy paragraph is trying to address. Unclear what is unclear? This paragraph is discussing bypassing of authentication requirements.

Page 23

4.1.2 I noted that minimum password length is 8 characters. Good. 2nd paragraph states that passwords will be distributed in a secure manner, but fails to define or explain what that means. Same with policy on positively identifying a user before providing temporary passwords. Procedure, not policy By saying any password transmission or storage will be encrypted to prevent capture is good, but transmission by what means, email, telephone, fax???

As long as it is encrypted, any means of transmission is valid.

Procedure, not policy

Page 25, Bullet 2 does not provide a maximum number to establish a standard. Procedure, not policy Bullet 4 talks about an employee, but not contractors. Agreed –

will add. 1st paragraph talks about the SSP, so call it that, not some nebulous document. Agreed – will change. This paragraph then jumps around talking about user access, security administrators (who are not mentioned at all in roles and responsibilities or how they fit into the program, or who they are) and fails to identify who is authorized to by-pass controls, whether written justification is required etc... Procedure, not policy

2nd paragraph. Absolutely wrong. The system manger cannot make these decisions alone. They MUST get approval from the system owner and DAA to effect such fundamental changes in a systems security posture. this section needs to be rethought and corrected Agreed – again, this was done before C&A guidance was complete. Will rewrite to reflect current necessary approvals.

4.2.1 The system manager and the SSO should select the security administrator so just do that here. Procedural, and may not be sys admin. System personnel reviewing the ACL every 6 months is not often enough if a viable user management process is used. Every other month or monthly at a minimum is best; six months would be an absolute maximum. True, that was why we used “at least”. Removal standard here contradicts your policy stated before which calls for immediate removal of accounts when staff leave. You need to resolve this. The six months is the standard for a review to determine any missed invalid users. This review is in order to catch any possible accounts missed for whatever reason from an immediate removal.

Page 26, 4.2.2 This section does not adequately address warning banners requirements. Does General Council need to approve the banner? What does it have to say or can they make their own up? See section 4.1.1 It mentions unauthorized disclosure but does not address unauthorized access. (Assuming this is in regards to second paragraph sentence about Privacy Act information) Privacy Act consequences to a user pertain to unauthorized disclosure, not unauthorized access. The rest of the section covers restricting access to authorized users.

4.2.3. **This policy is wrong.** System managers should not approve telecommuting connections without the employees’ supervisor first approving the request for work at home. Agreed – will add. This policy also does not address how security will be implemented for dial in/remote access. that is what this section is supposed to address. Procedure, not policy What about security at the users end? What policies apply to home users? See section 2.4 (Rules of Behavior) Who is responsible for that and who can direct measures be implemented to protect FSA data at the users end? This is also not addressed. Procedure, not policy

4.3 the second sentence contradicts the first. No one is supposed to even view audit logs except those authorized, especially the security logs. Agreed – will change “anyone” to “authorized security personnel”. Authorization to view must be approved in writing by the SSO. Agreed – will add. Also this policy only requires logs to be reviewed AFTER an incident or known violation. This is counter to best practice doctrine. This also violates Department policy and standards that will require log review weekly. Agreed – will add “or at least weekly”. This policy section needs to be redone.

Bullet 1 should include directories as well as files Agreed – will add.

Page 27, paragraph 1, Audit clocks need to be synchronized, but so do machine clocks as well, or are they one and the same? This is critical to note if you are transferring sys logs to a sys log server from another machine. The clocks across the enterprise must be synchronized. Agreed – will make changes.

Paragraph 2. Why does the SSO need to notify the user that keystroke monitoring is being used? If your warning banner is legal and correct this is not necessary. Why does Department of Justice need to review ED policy? That is what our General Council is for. This needs to be changed Need to check source requirements.

Last paragraph does not belong here; it belongs in the separation of duties section. Disagree – this relates directly to system auditing.

Page 24, 4.1.3 The system manager is not to grant waivers without the consent of the system owner and DAA. By doing so you can forfeit the C&A of the system in a heart beat! Remove this from the policy, or correct it to say the system owner must approve the waiver. Agreed – will change. In the case of contractor use, it could impact contractual requirements as well. The last sentence introduces PIN numbers, but that is not what the section is addressing. Also, if PINs are used, what is the standard? PIN generators?, self selecting by users,,what? Procedure, not policy.

4.2, line 2 needs to add the words "...and log..." to the sentence. Agreed – will add.

25-32 Roles and Responsibilities. Many of these do not track back into in the document and visa versa. Agreed – this section was not updated with the rest of the document; however, roles and responsibilities are, at heart, a procedural matter. We will remove this table. No one is responsible for incident handling. Half the responsibilities of the system manager as stated in the policy document are not included in the matrix. Some specific examples of these problems are:

The FSA CIO cannot establish Privacy policy as this implies. That is the responsibility of the ED Privacy Act official. If FSA specific policy is required, the ED Privacy Act official must approve it.

The CIO cannot grant authority to operate and be the certifier, this is a conflict of interest and counter to NIST standards in C&A.

CSO, Bullet 8 is wrong. C&A is to be coordinated with system owners AND system managers.

The roles of Functional manager fall far short and do not include their role in the C&A process

System managers: The last sentence under the position contradicts your policy of who can authorize access to FSA systems. Bullet 9 is not the system manager's call in most cases. The decisions must be made by the DAA.

System Security Officer. These listed duties are not supported by the policy; in fact the SSO is left out of the policy statements that cover these duties.

System Admin. As written the duties are a conflict of interest and would not pass the test of separation of duties policy. Re name the role as security administrator and it would be better.

System Developer: Bullet 4 is a direct conflict of interest and violates the stated FSA policy on separation of duties. Bullet 6 contradicts the policy regarding use of live data for testing.