

## FSA Risk Assessment Overview

System Name	Contractor	Number of Findings	Risk Finding Breakdown	General Comments
PELL	BAH	6	High - 2 Medium - 4 Low - 0	
VDC	BAH	6	High - 1 Medium - 4 Low - 1	No assessment of applications (non-MA) operated at VDC
IFAP	BAH	10	High - 1 Medium - 8 Low - 1	
SAIG	BAH	6	High - 0 Medium - 3 Low - 3	
NSLDS	BAH	3	High - 0 Medium - 3 Low - 0	
DLCS	BAH	7	High - 2 Medium - 5 Low - 0	
FFEL	BAH	4	High - 0 Medium - 4 Low - 0	
CPS	BAH	9	High - 1 Medium - 7 Low - 1	
OCTS	BAH	6	High - 0 Medium - 2 Low - 4	
PEPS	Spectrum Systems	16	High - 7 Medium - 6 Low - 3	Followed FSA methodology and actually improved on the reporting format. Traceable risk analysis and clear prioritization.
DLSS	D&T	50	High - 13 Medium - 18 Low - 19	Some findings are repeats. RA did not consolidate findings from various facilities.
DLOS	PwC	10	High - 1 Medium - 6 Low - 3	

## **Executive Overview of Department's Assessments of 9 FSA systems**

1. Why did BAH not validate controls of Major Applications housed at least partially at the VDC? In the executive summary of several of the assessments, the assessor states that resource limitations prohibited the team from validating controls at the GSS. This statement is questionable. The assessor had a team at the GSS to review the GSS's security controls. It seems logical that, while doing the GSS assessment, the team could have validated several of the MA controls as well. The ability to do this very action was supposed to be one of the benefits of having a single contract perform the majority of our risk assessments. They had the ability to validate them. The assessments continue, stating that, "system owners, managers, administrators, and/or developers have assumed that the host GSS Virtual Data Center (VDC) or other infrastructure resources would provide security services to meet these requirements. This assumption should be examined for validity." Who exactly, beyond a team of assessors, should examine the statement's validity?
2. In some of the assessments, the name and title of those interviewed were given. In others, only the title. However, not one of the assessments provided a summary of the interviews conducted. It is considered a best practice to provide the name, title, and contact information of the person interviewed as well as the date and location of the interview. Additionally, the interview summary should contain a list of the questions asked and ideally a summary of the interviewee's responses. This information is then used as a justification for compliance/non-compliance with BLSR elements. These interview results are then used as a basis for Certification testing during the Certification and Accreditation process. Without the results of the interviews, the system owners must re-interview the system personnel to baseline the Certification tests.
3. The assessments show incomplete or nonexistent justification for likelihood and impact assessments. It appears as though the assessments are based loosely on matrices included in the assessments and the interpretation of the individual assessor. For example, there is little documentation to describe/trace what area of sensitivity (confidentiality, integrity, availability) the threat/vulnerability pair may affect. This information is helpful when trying to design mitigation plan to improve the security controls on a system (which was the general purpose of the risk assessments).
4. Were the controls in the BLSR tested? How was each of the 106 BLSR elements verified? With no traceable documentation to build on for the next assessment and C&A, the system owners will be forced to re-conduct interviews, system tests and site inspections for every BLSR element. Effectively, based on these reviews, the system owners have not advanced their system assessment requirements and will again have to start from the beginning for their next assessment.