

16 September 2003

MEMORDANUM FOR AFAA/FSS
(ATTN: J. STARK, D. EDSELL)

FROM: SAF/IEBB
PENTAGON, DC

SUBJECT: Interim Results, Base Realignment and Closure Data Collection System (Project F2003-FB4000-0924.000)

1. Reference your memoranda, 4 September 2003, same subject. I would like to express my thanks to your folks for providing the interim results forward on 4 September 2003. The observations of the Audit Agency have proved to be helpful in guiding our development team to a successful deployment of the WIDGET application. AFAA's expected, continued support of our efforts during BRAC 05 execution is appreciated.

2. The following comments are made regarding each of the observations:

a. The WIDGET requirements have not been adequately documented. The available documentation is incomplete; fails to identify measurable specifications; and does not describe application risks and security measures.

(Comment): Requirements for the application will be adequately documented with the publication of the development and management plan. Expected date for publication is 19 SEP 03

b. The WIDGET test plan lacks details on the functions to be tested. The test acceptance level has not been identified.

(Comment): Test plan and acceptance level will be included in the development and management plan. Expected date for publication is 19 SEP 03

c. Because of incomplete documentation and programming, we have not been able to determine whether adequate audit trails are created or maintained.

(Comment): This observation is not understood. However, the processes for completing the data gathering at all levels is contained in the user's guide and it documents the methods to be used in answering questions, making changes, tracking the data gathering process up to and including the HAF level, and providing requirements for collection and retention of documentation associated with answers. In addition, the automated portion of the auditing/tracking process within WIDGET is captured in the requirements for the application. The user's manual will be incorporated as an Appendix to the development and management guide. Expected date for publication is 19 SEP 03

d. Because of incomplete documentation and development, we have not been able to determine the security and certification planned. However, we noted:

i. Specific requirements for encrypting user passwords have not been established.

(Comment): There is no requirement to encrypt passwords for the user community. The

passwords are maintained within the database server environment and are only legitimately accessible by a limited number of trusted agents of the AFPCA. Although this is not an issue, the recommendation of the auditor has been determined to be of value and we will determine the feasibility of encrypting passwords to enhance security.

ii. Secure socket layer using 128-bit encryption was not specified in the documentation Limiting WIDGET web page logon to “.Mil” addresses was not specified in documentation.

(Comment): The 128-bit SSL is a user requirement to obtain access to the web site hosted by AFPCA. This is an AFPCA requirement and as such is not reflected in the development and management plan for WIDGET. The same can be said for the domain limitation to those accessing the web-site (AFPCA) as identifiable as coming from a ‘.mil’ IP address. These two items are addressed in the accreditation, certification and operating documentation for the AFPCA web environment. However, both of these will be reiterated as necessary in the agreement between AFPCA and SAF/IEBB for the hosting of WIDGET.

iii. Separation of duties for question answerer and reviewer has not been established. GAO internal control standards state “Key duties and responsibilities need to be divided or segregated among different people to reduce the risk of error or fraud.”

(Comment): The Air Force Internal Control Plan does not state a requirement to have two different individuals perform the activity of answering a question and approving the input (answerer and reviewer) at the installation level. With three separate and distinct layers of review and accreditation of the answer to a question, there is an extremely low probability that contrived answers, inaccurate inputs, or misinformation will flow through to analysis. This low probability and associated impact are acceptable risks. In addition, installation commanders must have the latitude to delegate responsibility for BRAC activity to the level necessary for his/her assurance of complete and accurate data, and commensurate with available resources.

iv. Restrictions on access to privileged programs on servers were not established.

(Comment): The restrictions on access to privileged programs are contained in the standard operating instruction of AFPCA. The one privileged program associated with WIDGET is the ORACLE database and its associated server. Current AFPCA policy only allows 3 individuals to have the credentials to access this software and its associated WIDGET partition on the database server. Each of the individuals occupies a position of trust in AFPCA and must meet AFPCA criteria for appointment and performance. This represents an acceptable level of risk to data integrity for this application.

v. Data sensitivity and mission criticality have not been formally identified.

(Comment): These are well defined within the Air Force Internal Control Plan for BRAC 2005. In addition the Risk Management Plan (Appendix F to the proposed Development and Management Plan) identify and evaluate the risks associated with data sensitivity and criticality. Publication and maintenance of the RMP will ensure acceptable levels of risk;.

vi. The AFPCA backup and recovery procedures have not been evaluated to determine if BRAC requirements will be met.

(Comment): Discussion with AFPCA indicates that their methods of backup, recovery and archiving physical storage devices are adequate for the WIDGET application. This will be reiterated as an ‘understood’ in the host/customer agreement between AFPCA and SAF/IEBB to ensure the understanding is well known between the two activities. The

host/customer agreement is in Appendix E to the development and management plan.
Expected date for publication is 19 SEP 03

3. My focal point for WIDGET application development and deployment is Mr. Martin Bullock, martin.bullock@pentagon.af.mil, DSN 222-5122. Please contact him concerning any issues with the audit of this application.

//Signed, 16 Sep 03//
THOMAS FLEMING, Colonel, USAF
Chief, Base Realignment and Closure Division