

# AIR FORCE AUDIT AGENCY



## BASE REALIGNMENT AND CLOSURE DATA COLLECTION SYSTEM

This document contains information exempt from mandatory disclosure under the Freedom of Information Act. Exemption 5 applies.



# AUDIT REPORT

F2004-0008-FB4000

27 September 2004

**FOR OFFICIAL USE ONLY**

Deliberative Document – For Discussion Purposes Only

Do Not Release Under FOIA

## Executive Summary

---

### INTRODUCTION

Public Law (PL) 101-510, the Defense Base Closure and Realignment Act of 1990, as amended, establishes the exclusive procedures under which the Secretary of Defense may pursue the closure or realignment of major military installations inside the United States, its territories, and possessions. The Deputy Assistant Secretary of the Air Force (Basing and Infrastructure Analysis) (SAF/IEB) is responsible for Base Realignment and Closure (BRAC) data collection and analysis. The Air Force BRAC 2005 Internal Control Plan establishes management controls designed to provide an “unbroken chain” of accountability for information and analysis used in the Air Force BRAC 2005 process. Data collection for the base questionnaire will be accomplished via a web-based data collection application identified as the Web-based Installation Data Gathering and Entry Tool (WIDGET).

### OBJECTIVES

Our overall objective was to determine whether WIDGET met BRAC reliability and accuracy requirements. Specifically, we determined if management:

- Fully tested requirements.
- Created and maintained audit trails.
- Developed adequate security and certification processes.
- Established data collection system requirements for reliability and accuracy.

### CONCLUSIONS

We determined that, as designed, the BRAC data collection system should meet the goal of providing an unbroken chain of accountability for installation information. Management tested identified requirements, including audit trails, prior to operational use, and completed WIDGET certification in April 2004. However, management chose not to establish requirements for system data accuracy, or document the re-test of software changes. Also, management elected not

## **Executive Summary**

---

to include all available security procedures but instead accepted the increased risks. Specifically:

- WIDGET managers did not establish accuracy requirements for the WIDGET data collection system. Establishing accuracy requirements permits developers and users to review solutions and test processes against mission needs. (Tab A, page 2)
- Although all identified WIDGET requirements were tested, management did not document the follow-up testing conducted to verify that corrective actions effectively resolved software problems. Without documented test results, neither management nor audit could effectively evaluate WIDGET software changes. (Tab A, page 3)
- Although WIDGET managers identified many security features as requirements and adequately tested them, management did include other important security features. Management accepted the risks of not including these procedures. (Tab B, page 7)
- WIDGET allowed reviewers to assign questions to themselves as answerer, eliminating separation of duties. Management accepted the risk inherent in not having this control. (Tab B, page 7)

**RECOMMENDATIONS** We made one recommendation to SAF/IEB to test and document application changes before operational use. (Reference the individual Tabs for specific recommendations.)

## Executive Summary

---

### MANAGEMENT'S RESPONSE

Management officials agreed with the audit results and recommendation contained in this report. Management corrective actions planned are responsive to the issues and recommendation included in this report.



VALERIE L. MUCK  
Associate Director  
(Information Systems Security and Communica-  
tions Division)



DONNA L. EDSALL  
Assistant Auditor General  
(Financial and Systems Audits)

## Table of Contents

---

	<u>Page</u>
<b>EXECUTIVE SUMMARY</b>	
<b>TAB</b>	
<b>A Requirements</b>	
<b>B Internal Controls</b>	
<b>APPENDIX</b>	
<b>I Background Information</b>	
<b>II Audit Scope and Prior Audit Coverage</b>	
<b>III SAF/IEB Memorandum, October 2003</b>	
<b>IV SAF/IEB Memorandum, February 2004</b>	
<b>V Locations Audited/Reports Issued</b>	
<b>VI Opinion of C. fact</b>	<b>21</b>
<b>VII Final Report Distribution</b>	<b>23</b>

# Tab A

## Requirements

---

### SYNOPSIS

The BRAC 2005 Division (SAF/IEBB) WIDGET system program office did not establish accuracy requirements. This occurred because program managers believed using commercial software eliminated the need to establish accuracy requirements. Establishing accuracy requirements permits developers and users to review solutions and test processes against mission needs.

Although all identified WIDGET requirements were tested, management did not document the follow-up testing conducted to verify that corrective actions effectively resolved software problems. This occurred because of time constraints. Without documented test results, neither management nor audit could effectively evaluate WIDGET software changes.

### BACKGROUND

The Air Force BRAC 2005 Internal Control Plan (ICP) establishes management controls designed to provide an “unbroken chain” of accountability for each information and analysis sub-element used in the Air Force BRAC 2005 process. The goal is to ensure the accuracy, completeness, and integration of all information and analytical processes upon which the Secretary of the Air Force’s BRAC 2005 recommendations to the Secretary of Defense are based. The following Air Force regulations provide additional guidance for establishing accuracy requirements and testing.

- Air Force Instruction (AFI) 33-101, *Communications and Information Management Guidance and Responsibilities*, 24 July 1998, requires all command levels to “provide specific performance-based requirements” in system development documents.
- Air Force Directory 33-303, *Compendium of Communications and Information Terminology*, 1 February 2002, defines automated information systems accuracy as being “free from error. Accuracy denotes the absolute quality of computed results. In contrast, precision refers to the degree to which computed results reflect theoretical values.”
- Air Force Manual (AFMAN) 99-111, *Command, Control, Communications, Computers and Intelligence (C4I) Test and Evaluation Process*, 1 March 1996, states: “without an effective software test and evaluation effort, the software, and therefore the system has unmanaged risk.”

## Tab A Requirements

---

The Air Force Base Questionnaire is the primary means of collecting data for use in the BRAC process. Data collection for the base questionnaire will be accomplished through a web-based data collection system -- the WIDGET. This tool is a software application composed of web-based screens and database structures, which allow users to input, review, and certify data for use during BRAC analysis processes.

### **AUDIT RESULTS 1 – RELIABILITY AND ACCURACY**

**Condition.** Although the SAF/IEBB system program office established reliability requirements for WIDGET, system documentation did not specify a minimum acceptable accuracy level. While the system documentation did not contain an accuracy standard, SAF/IEBB tested the system reliability and accuracy in May 2004 and determined WIDGET was adequate to reliably and accurately accept, store, and reproduce user-entered data.

**Cause.** This condition occurred because WIDGET applications use commercial off-the-shelf software operated by the Air Force Pentagon Communications Agency (AFPCA), and the program manager believed “it would be redundant to attempt to establish the same requirement within the WIDGET management and development plan.”

**Impact.** Documented accuracy requirements permit developers and users to review solutions and test processes against mission needs. Without established requirements, any level of accuracy obtained could appear acceptable, and could hinder the Air Force from achieving its goal of ensuring accuracy and completeness of BRAC data.

**Management Action.** We briefed SAF/IEB on 10 December 2003 on the need for accuracy requirements. On 2 February 2004, SAF/IEB provided a memorandum, *Attaining Reliability and Accuracy within the Web-based Installation Data Gathering and Entry Tool (WIDGET)*.<sup>1</sup> SAF/IEB stated: “It is my determination that we have met and will meet the intended requirements goal of reliability and accuracy [in the ICP]. I am confident that the selection of approved software products and the use of the operational capability of the network service provided by [AFPCA] meet or exceed the criteria to obtain and protect BRAC information throughout the collection phase. The use of these standard products, within the accredited AFPCA environment, lends the maximum attainable accuracy to the automated process commensurate with WIDGET requirements.” In

---

<sup>1</sup> See Appendix III for a copy of the memorandum.

addition, SAF/IEBB tested the reliability and accuracy of WIDGET in May 2004 with satisfactory results.

**Audit Comment.** While we believe management should have documented accuracy requirements for data input, storage, and retrieval before the system was placed in operational use, the subsequent testing validated WIDGET accuracy and reliability capabilities. Therefore, we are not making any recommendations.

**Management Comments.** SAF/IEB concurred with the finding and audit comment.

## AUDIT RESULTS 2 – TESTING

**Condition.** Although all identified WIDGET requirements were tested, management did not document follow-up test results conducted to verify that corrective actions effectively resolved all software problems. We identified 52 requirements in WIDGET project documents that we successfully traced to WIDGET test results contained in the operational test report and the completed test scripts of user functions such as logon, change passwords, and print documents. However, the operational test report stated that, although the overall test results were positive, two significant errors or problems warranted further attention:

- During the test, while sections appeared to be locked, major command (MAJCOM) and Headquarters Air Force (HAF) Points of Contact (POCs) could, in fact, still edit (change) answers. While this deficiency did not prevent certification of the answers provided, it also did not prevent an answer from being changed after the answer was locked but not yet certified.
- During the test, some MAJCOMs and installations bypassed assigning sections to functional expert POCs and instead assigned questions directly to the answerers. This process was not standard and not recommended because a functional expert POC did not review the answers as prescribed in the Air Force BRAC 2005 ICP.

To resolve the locking section error, the test report stated a software modification was required with an estimated completion date of 31 October 2003. To resolve section assignment issues, management modified the question-level assignment option to require functional POC reviewer assignment. However, management did not document test results for these changes although WIDGET development personnel said they made the changes. In addition, management did not provide audit with test results for three installed software patches identified in the on-line WIDGET trouble ticket listing.

## Tab A Requirements

---

**Cause.** The WIDGET program manager did not supply complete system test documentation, including re-test results, because of time constraints.

**Impact.** Without documented test results, neither management nor audit could effectively evaluate the changes made to the WIDGET software. Potentially, these changes to the WIDGET software could adversely affect application processes or program controls. For example, WIDGET on-line trouble tickets indicated the answer locking problems continue to occur in the operational system. Documented software changes and test results also facilitate making future system modifications.

**Recommendation A.1.** SAF/IEB should require the WIDGET system program office to:

- a. Update WIDGET documentation with test results for all software changes made since the previous test reports.
- b. Document testing of all future software changes before placing the changes into operational use.

**Management Comments.** SAF/IEB concurred with the finding and recommendation and stated:

- a. “Concur. SAF/IEB will ensure Attachments to Appendix H (Test) of the Management and Development Plan are included to identify tests and results as they are completed. Appending Attachments for tests to date will be completed by 30 September 2004.
- b. “Concur. SAF/IEB will ensure Chapter 5 (Test) of the Management and Development Plan is updated to include guidance on identifying required tests and posting test results as an Attachment to Appendix H. Change will be completed by 30 September 2004.”

**Evaluation of Management Comments.** SAF/IEB comments and planned actions are responsive to the findings and recommendation.

## Tab B Internal Controls

---

### SYNOPSIS

(FOUO) The WIDGET system program office security processes did not include all available procedures.<sup>2</sup> SAF/IEBB determined that exceptions to Air Force standard security procedures were “within acceptable limits of risk for the level of effort and intent of WIDGET.” As a result, the BRAC data in WIDGET was not optimally protected.

SAF/IEBB design of WIDGET allowed reviewers to assign questions to themselves as answerer, eliminating separation of duties. This occurred because SAF/IEBB believed installation commanders must have the latitude to delegate responsibility for BRAC activity commensurate with available resources. Not separating duties increases the risk that inaccurate inputs or misinformation could be used in BRAC analysis. SAF/IEB accepted the increased risks associated with not incorporating these controls in WIDGET.

### BACKGROUND

The Comptroller General has issued Standards for Internal Control in the Federal Government.<sup>3</sup> These standards include segregation of duties -- key duties and responsibilities need to be divided or segregated among different people to reduce the risk of error or fraud. This should include separating the responsibilities for authorizing transactions, processing and recording them, reviewing the transactions, and handling any related assets. No one individual should control all key aspects of a transaction or event.

Program managers and software developers must integrate information assurance into their systems using guidance contained in relevant Air Force publications. AFI 33-202, *Network and Computer Security*, 26 September 2003, contains Air Force primary computer security (COMPUSEC) guidance. The objectives of COMPUSEC are to protect and maintain the confidentiality, integrity, availability, authentication, and nonrepudiation of information system resources and information processed throughout the system's life cycle. In addition, COMPUSEC procedures safeguard information systems and

---

<sup>2</sup> WIDGET security features include minimum password composition requirements, limiting access to “.mil” domain users, and using secure socket layer encryption (128-bit). However, features such as changing passwords every 90 days and encrypting the password file, were not established.

<sup>3</sup> United States Government Accountability Office, Standards for Internal Control in the Federal Government, GAO/AIMD-00-21.3.1, November 1999.

## Tab B Internal Controls

---

information against tampering, denial of service, fraud, misuse, or release to unauthorized persons. Specific security features include:

Using passwords with at least eight alphanumeric characters (upper and lower case) with at least one special character (@&+, etc.).

Changing passwords every 90 days.

- Limiting the number of attempts allowed for correct password entry. Normally three attempts are permitted.
- Following a successful log-in procedure, informing the user of the last successful access to the account and of any unsuccessful intervening access attempts.
- Restricting web pages to selected users by accepting connections from internet protocol addresses ending in “.mil” or “.gov” only.
- Using web servers having 128-bit Secure Sockets Layer (SSL) encryption.

SAF/IEBB provided the Air Force Communications Agency (AFCA) information to support the WIDGET certificate of net worthiness. On 28 October 2003, AFCA issued a “certificate of net worthiness with timed conditions”<sup>4</sup> and on 20 April 2004 AFCA issued the final certificate. In addition, the AFPCA commander issued WIDGET a certificate to operate on 8 February 2004.<sup>5</sup>

The Air Force BRAC 2005 ICP defines different roles for “answerer” and “reviewer.” Specifically,

- The answerer is the person at the installation who initially answers the question (assigned access code for specific question page), and may not necessarily be the source of information.

<sup>4</sup> An interim approval to use the system until a specified date so that management can implement required changes.

<sup>5</sup> The AFPCA is a field operating agency responsible for acquiring, operating, and maintaining communications, information systems, and computer system services critical to national defense for the Office of the Secretary of the Air Force, HAF, and other organizations.

- The reviewer is any person assigned, at any level, to review and approve the accuracy of the answers to the questions on the base questionnaire.

### **AUDIT RESULTS 3 – SECURITY PROCEDURES**

**Condition. (FOUO)** The WIDGET system program office security processes did not include all available procedures. WIDGET developers identified some security features<sup>6</sup> as requirements, included these in the application design, and tested the features before operational use. However, the system program office did not require other important security features, such as changing passwords every 90 days (or for every data call as a surrogate) or limiting failed logon attempts before an account was locked. In addition, the WIDGET user password file in the database was not encrypted on the server. These weaknesses were compounded by other system processes (e.g., allowing multiple, simultaneous user logons and not providing users information regarding their last logon).

**Cause. (FOUO)** The WIDGET system program office determined that exceptions to Air Force standard security procedures were “within acceptable limits of risk for the level of effort and intent of WIDGET.”

**Impact. (FOUO)** As a result, the BRAC data in WIDGET was not optimally protected.

**Audit Comment. (FOUO)** We briefed SAF/IEB on 10 December 2003 regarding the Air Force security procedures not incorporated into WIDGET. Management revised WIDGET documentation accepting the increased risks associated with not incorporating these procedures. Based on SAF/IEB identification and acceptance of the risks, we are making no additional recommendations.

**Management Comments.** SAF/IEB concurred with the finding and audit comment.

### **AUDIT RESULTS 4 – SEPARATION OF DUTIES**

**Condition.** The SAF/IEBB system program office design of WIDGET allowed reviewers to assign questions to themselves as answerer, eliminating separation of duties.

---

<sup>6</sup> Features such as minimum password composition requirements, limiting access to “.mil” domain users, and using SSL encryption (128-bit).

## Tab B Internal Controls

---

Allowing “reviewers” to assign themselves as “answerer” eliminates the separation of duties inherent in these positions.<sup>7</sup>

**Cause.** SAF/IEBB believed “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.”

**Impact.** Lack of separation of duties increases the risk that inaccurate inputs or misinformation could be used in BRAC analysis.

**Audit Comment.** We provided our evaluation to SAF/IEBB in September 2003. In a memorandum dated 2 October 2003, SAF/IEB reflected on all arguments and decided to accept the risks identified and to manage the risk based on a risk mitigation strategy.<sup>8</sup> Based on SAF/IEB identification and acceptance of the risks, we are making no additional recommendations.

**Management Comments.** SAF/IEB concurred with the finding and audit comment.

**Evaluation of Management Comments.** SAF/IEB comments are responsive to the issues identified.

---

<sup>7</sup> This is similar to the condition reported in Tab A, Audit Results 2, where BRAC points of contact circumvented separation of duties by directly appointing answerers without any reviewers.

<sup>8</sup> See Appendix IV for a copy of the memorandum.

## **Background Information**

---

### **DEFENSE BASE CLOSURE AND REALIGNMENT ACT**

Part A, Title XXIX of PL 101-510, the Defense Base Closure and Realignment Act of 1990 (DBCRA), as amended, establishes the exclusive procedures under which the Secretary of Defense may pursue the closure or realignment of major military installations inside the United States, its territories and possessions, until April 15, 2006. Consistent with the law, the Secretary of Defense has directed that base closure, realignment, or consolidation studies must be based on the force structure plan required by Section 2912 of the DBCRA; final criteria, established by the Secretary of Defense, for recommending bases for closure and realignment under Section 2913 of the DBCRA; and consider all military installations inside the United States and its territories, not previously selected for closure, on an equal footing without regard to prior consideration for closure or realignment.

### **AIR FORCE INTERNAL CONTROL PLAN**

The Secretary of Defense has also directed that DoD components establish internal control plans for base realignment and closure or consolidation studies to ensure the accuracy of data collection and analyses. The Air Force BRAC 2005 ICP establishes management controls designed to provide an “unbroken chain” of accountability for each sub-element of information and analysis used in the Air Force BRAC 2005 process. The goal is to ensure the accuracy, completeness, and integration of all information and analytical processes upon which the Secretary of the Air Force’s BRAC 2005 recommendations to the Secretary of Defense are based, and to limit the possibility of premature disclosure of BRAC 2005 information.

### **AIR FORCE DATA COLLECTION STRUCTURE**

The SAF/IEB is responsible for BRAC data collection and analysis. The division is responsible for data gathering including developing an automated information system to gather and store installation information.

The Air Force Base Questionnaire is the primary means of collecting data for use in the base realignment and closure process. Data is collected from the organizational level commensurate with the question. Normally, this begins at base level. Review and certification should be accomplished as prescribed within the context of the question and chain of command. All BRAC data must be certified up to and including the HAF level.

Data collection for the base questionnaire will be accomplished via a web-based data collection tool. The data collection tool is the WIDGET. This tool is a software applica-

## Background Information

---

tion composed of web-based screens and database structures, which allow users to input, review, and certify data for use during BRAC analysis processes. Use of this tool will ease the data collection, review, and certification process and reduce requirements for handling, mailing, and storage of large volumes of paper during BRAC 2005.

## REVIEW CRITERIA

Our review was based on Title XXIX of PL 101-510, the Defense Base Closure and Realignment Act of 1990, as amended; the Comptroller General's Internal Control Standards;<sup>9</sup> and the Air Force BRAC 2005 ICP. In addition, the following Air Force directives and regulations were used in the evaluation.

- AFI 65-201, *Management Control*, 1 May 1997, states assuring that proper controls, manual or automated, are in place in automated systems is an important aspect of the Management Control program.
- AFI 33-114, *Software Management*, 1 July 2000, states program managers and software developers must integrate information assurance into their systems using guidance contained in AFD 33-2, *Information Protection* (converting to *Information Assurance*), and other relevant Air Force guidance.
- AFI 33-202, *Network and Computer Security*, 26 September 2003, implements the Air Force COMPUSEC Program.
- AFMAN 33-223, *Identification and Authentication*, 21 November 2003, addresses and defines security features. "Identification" is the process where individuals identify themselves to a system as a valid user. "Authentication" is the procedure where the system verifies the user has a right to access the system. User identifications (user-ID) and passwords, because of their cost-efficiency and ease of implementation, are the most common identification and authentication methods. Because of their vulnerability to interception or inadvertent disclosure, they are also the weakest of methods.
- AFI 33-129, *Transmission of Information Via the Internet*, 4 April 2001, provides the following guidance:

---

<sup>9</sup> United States Government Accountability Office, Standards for Internal Control in the Federal Government, GAO/AIMD-00-21.3.1, November 1999, page 14.

## Background Information

---

Information approved for limited release must have added safeguards and security controls to limit access by other internet users. Restrict pages and bulletin boards to selected users by accepting connections from internet protocol addresses ending in “.mil” or “.gov” and/or by requiring a password.

Server Certificate. In accordance with Assistant Secretary of Defense, Command, Control, Communications, and Intelligence August 12, 2000 Memorandum, Subject: “Department of Defense (DoD) Public Key Infrastructure (PKI), Management and Use,” all private Air Force web servers must be issued a DoD X.509 PKI Server Certificate and have 128-bit SSL using this certificate enabled at all times.

- AFMAN 99-111, *Command, Control, Communications, Computers and Intelligence (C4I) Test and Evaluation Process*, 1 March 1996, states without an effective software test and evaluation effort, the software, and therefore the system, has unmanaged risk. Software testing must be conducted in accordance with written test plans and procedures.

We also used the Service Level Agreement between HAF and AFPCA, 19 November 2001, to identify responsibilities for operating computer networks and applications. AFPCA operating instructions further explained responsibilities for hosting HAF applications. Finally, we used the Air Force BRAC Operating Instruction 04-1, *Guidelines for BRAC Data Calls*, 1 December 2003.

**This Page Intentionally Left Blank**

## Audit Scope and Prior Audit Coverage

---

### AUDIT SCOPE

**Audit Coverage.** We performed this review at the office of SAF/IEB, AFPCA, and HQ USAF Deputy Chief of Staff, Installations and Logistics, Directorate of Communications Operation (AF/ILC). We evaluated WIDGET development and testing requirements, concepts, and documentation.

To determine if reliability and accuracy requirements had been established, we made inquiries of the program manager, reviewed WIDGET documentation, and briefed SAF/IEB.

- To determine if WIDGET requirements were tested, we:
  - Listed requirements, based on 18 November 2003 project documents, and cross indexed to tests performed.

Reviewed test scripts and functional tests performed and evaluated test results.

- Performed on-line tests of logon, navigation, and audit trails.

Requested documentation for software changes made as a result of functional tests.

- To determine if WIDGET audit trails existed, we:

Identified audit trail requirements, based on 18 November 2003 project documents, and cross-indexed to tests performed.

Reviewed test scripts and functional tests performed and evaluated test results.

Performed on-line tests of logon, navigation, and audit trails.

- To determine the adequacy of WIDGET security and certification processes, we:

Held discussions with SAF/IEBB personnel and AFPCA personnel

## Audit Scope and Prior Audit Coverage

---

Reviewed WIDGET project documents.

- Reviewed AFPCA policies and procedures.
- Reviewed security scans performed by AFPCA on servers.

Reviewed the DoD Inspector General memo on information technology security and made inquiries regarding any Office of the Secretary of Defense BRAC policy.

We performed fieldwork from August 2003 through May 2004, and reviewed documents dated from June 2000 through May 2004. We provided a draft report to management in June 2004.

**Sampling Methodology.** We did not use statistical or judgmental samples or computer assisted auditing tools and techniques to analyze data or project results in this audit.

**Data Reliability.** We did not rely on computer-generated data to support conclusions in this audit.

**Auditing Standards.** We conducted the audit in accordance with generally accepted government auditing standards and, accordingly, included tests of internal controls associated with system development and testing, audit trails, system access, and accreditation.

### **PRIOR AUDIT COVERAGE**

We did not identify any Air Force Audit Agency, DoD Inspector General, or Government Accountability Office reports issued within the past 5 years that addressed the same or similar objectives as this audit.

**SAF/IEB Memorandum, 2 October 2003**

True Copy



DEPARTMENT OF THE AIR FORCE  
WASHINGTON DC

OFFICE OF THE ASSISTANT SECRETARY

2 Oct 03

MEMORANDUM FOR AFAA/FSS (ATTN: MS EDSALL)  
5023 4<sup>th</sup> St  
March ARB CA 92518-1852

FROM: SAF/IEB  
1665 Air Force Pentagon  
Washington DC 20330-1665

SUBJECT: Review of AFAA Issue – Separation of Duties, BRAC 2005 Data Collection

On 30 Se 03 we discussed the issue of separation of duties within the Web-based Installation Data Gathering and Entry Tool (WIDGET) application associated with the BRAC 2005 Process. Based on our discussions I have decided to accept the identified risks.

My decision is based on the following salient facts:

a. The issue, as stated, concerns a GAO guideline for separation of duties, in general, when 'key duties and responsibilities need to be divided ... to reduce the risk of error or fraud'. The GAO guideline is well understood and it has been considered in this case. The counter argument, specific to WIDGET, is duties and responsibilities are well separated, because of the three separate layers of review and approval. These three layers are base-level, Major Command (MAJCOM) level, and Headquarters Air Force (HAF) level.

b. The GAO guideline tends to point towards activities that occur within an activity or work/cost center, such as a warehouse or a Squadron. On the other hand, the activities of WIDGET span across the total Air Force chain of command. For GAO we tend to think in terms of activities that are compartmented and without visibility in the sense of an outside review. On the other hand, data gathered via the WIDGET application is neither compartmented nor is it invisible to outside scrutiny. In fact, the application ensures open, visible and auditable collection of data across the Air Force, albeit by a limited number of individuals. In this case, I believe there are strong management responsibilities and we have instituted compensating controls to guard against error and fraud. These responsibilities are consummated by the Wing Commander at Base Level, the MAJCOM/CC (at the MAJCOM) and ultimately by the Secretary of the Air Force and the Chief Staff of the Air Force, with the advice and consent of the Assistant Secretary of the Air Force (Installations, Environment & Logistics).

I have reflected on all arguments and my decision is to accept the risks identified and to manage the risk based on the following risk management plan:

a. Risk Identification: Within the WIDGET application an individual, at the installation level, can perform the duties of providing an answer to a question or questions during the data gathering process. That same individual could be assigned the responsibility to review and

## SAF/IEB Memorandum, 2 October 2003

True Copy

2

approve the answer(s) he/she provided. Under the preceding circumstances, a risk does exist where error and/or fraud could be committed. Such error and/or fraud could go unnoticed during the data gathering process and that data could be used during analysis and therefore affect recommendations concerning closure or realignment.

b. Consequence: The consequence of utilizing erroneous and/or fraudulent data during analysis is grave. In addition, if this were a critical element of the analysis, such that it swayed a recommendation, it could, as worst-case scenario, negate recommendations formulated and presented by Air Force working groups, executive reviewing authority and the Secretary of the Air Force.

c. Risk Assessment. The probability of a critical element of data being used to formulate recommendations for closure or realignment is considered negligible. Although the situation is one that has less than optimal separation of duties at the installation level; as stated above, there are compensating controls in place as instantiated by the review and certification process within WIDGET. The balancing effect of the review and certification process provides a high level of confidence that an error and/or fraud, committed at the installation, will be found out.

d. Mitigation Strategy. Because of the consequence of this risk, SAF/IEB will mitigate the accepted risk using the following steps.

(1) Make a strong recommendation to all responsible offices for the separation of duties between answerer and reviewer at the installation level.

(2) Incorporate analysis, and provide reports, which identify an inordinate number of instances when the same individual is answering and reviewing questions. This will be shared with the appropriate MAJCOM with a recommendation to scrutinize those answers to ensure accuracy and correctness.

The recommendations and discussion provided by your office are greatly appreciated. Between our two activities I am confident that we will incorporate necessary controls and audit trails that will withstand scrutiny of our process.

//Signed//maa/SES/3 Oct 03  
MICHAEL A. AIMONE, P.E.  
Deputy Assistant Secretary  
(Basing & Infrastructure Analysis)

cc:  
SAF/AG  
AF/XP-2 (BRAC & QDR)

**SAF/IEB Memorandum, 2 February 2004**

True Copy



DEPARTMENT OF THE AIR FORCE  
WASHINGTON DC

OFFICE OF THE ASSISTANT SECRETARY

2 February 2004

MEMORANDUM FOR AFAA/FSS (ATTN: MS EDSALL)  
5023 4<sup>th</sup> St  
March ARB CA 92518-1852

FROM: SAF/IEB  
1665 Air Force Pentagon  
Washington DC 20330-1665

SUBJECT: Attaining Reliability and Accuracy within the Web-based Installation Data  
Gathering and Entry Tool (WIDGET)

After due consideration of the circumstances surrounding the development and operation of the subject tool, it is my determination that we have met and will meet the intended requirements goal of reliability and accuracy quoted in your latest status report. I am confident that the selection of approved software products and the use of the operational capability of the network service provided by the Air Force Pentagon Communications Agency (AFPCA) meet or exceed the criteria to obtain and protect BRAC information throughout the collection phase.

The WIDGET requirement for operational time and community access to the tool is consistent with the AFPCA web service availability that hosts WIDGET. The availability is reflected in the operational goal of AFPCA to provide 24 hour, 7 day a week, web accessibility through the HAF DMZ. This service is addressed in the Service Level Agreement between AFPCA and HAF. The reality of the situation is the rate of service is a goal and the web service will get interrupted by various and sundry consequences of simply operating a web site. The recovery requirement for WIDGET is consistent with the recovery requirements for the AFPCA environment. Therefore, the reliability provided by the AFPCA operational goals, recovery methods, and contingency plans are consistent with the reliability requirement for WIDGET. As this requirement is included in the operational documentation of AFPCA it would be redundant to attempt to establish the same requirement within WIDGET management and development plan.

Data accuracy is less a function of storage methodology than it is a function of the 9 layers of input/review/certification of the automated process. AFAA will tell me if these layers are sufficient to ensure the completeness and accuracy of the data collected. The Commercial Off the Shelf software products, which provide entry, transmission and storage of data, have been proven and are standard across the Air Force. The use of these standard products, within the accredited AFPCA environment, lends the maximum attainable accuracy to the automated process commensurate with WIDGET requirements.

## **SAF/IEB Memorandum, 2 February 2004**

---

True Copy

2

Accuracy of data extracted from that gathered during any particular data call, is a function of the operational system and the database engine. Again, these are standard and proven products, which are used across DOD. The risk of inaccuracy caused by the failure of one or both will be mitigated with the use of comparative file methodologies. The standards and practices used are consistent with established DOD-wide methodologies and do not deviate from time tested procedures.

The risks and consequences associated with WIDGET reliability and accuracy, as mitigated above, are known and acceptable.

The concern of AFAA in this matter is appreciated. Drawing this matter to my attention has caused this office to review all of our methodologies to ensure that issues raised have been addressed. My review has assured me that we are on the correct path during the data collection phase of the Air Force BRAC process.

//signed//tmaa/2 FEB 04  
MICHAEL A. AIMONE, P.E.  
Deputy Assistant Secretary  
(Basing & Infrastructure Analysis)

cc:  
SAF/AG  
AF/XP-2 (BRAC & QDR)  
AFPCA/CC

**Locations Audited/  
Reports Issued\***

---

**Organization/Location**

**Headquarters, U.S. Air Force**

SAF/IEB  
Pentagon, Washington DC

Air Force Pentagon Communications Agency  
Pentagon, Washington DC

\*We did not issue installation-level reports during this review.

## **Points of Contact**

---

Information Systems Security and Communications Division (AFAA/FSS)  
Financial and Systems Audits Directorate  
5023 4th Street  
March ARB CA 92518-1852

Valerie L. Muck, Associate Director  
DSN 447-4929  
Commercial (951) 655-4929

John W. Stark, Jr., Program Manager

Bartholomew Rice, Audit Manager

We accomplished this audit under project number F2003-FB4000-0924.000.

## **Final Report Distribution**

---

SAF/OS  
SAF/US  
SAF/FM  
SAF/IE  
SAF/IG  
SAF/LL  
SAF/PA  
AF/CC  
AF/CV  
AF/CVA  
AF/IL  
AF/JA  
AF/RE  
AF/XP  
NGB/CF

AU Library (AUL/LSE)  
DoD Comptroller  
GAO  
ODIG-AUD-DFS  
ODIG-AUD-FD  
OMB

### **FREEDOM OF INFORMATION ACT**

The disclosure/denial authority prescribed in AFPD 65-3 will make all decisions relative to the release of this report to the public.