

**Standing Operating Procedures for the
Headquarters and Support Activities Joint Cross-Service Group (HSA JCSG)
Base Realignment and Closure 2005**

1. Purpose.

This document contains important information on standing operating procedures related to controls necessary to safeguard the BRAC 2005 deliberative data, documents, decisions, and recommendations for the HSA JCSG.

2. Reference.

Memorandum, Under Secretary of Defense (Acquisition, Technology, and Logistics), 16 April 2003, subject: *Transformation Through Base Realignment and Closure (BRAC 2005) Policy Memorandum One – Policy, Responsibilities, and Procedures*. Includes Appendix B, *Office of the Secretary of Defense Internal Control Plan for the 2005 Base Realignment and Closure Process*.

3. Storage Requirements.

- a. Physical location used to store data. All BRAC 2005 data will be securely stored at the HSA JCSG Federal Government office space at 1401 Wilson Boulevard, Suites 400 and 501, Arlington, Virginia 22209.
- b. Physical security for the location. The entrance to the fourth floor office space is secured by a cipher lock on the door. The Security Manager will change the cipher lock combination on an as needed basis. The OSD BRAC Office Manager handles security for suite 501. Only the HSA JCSG staff will receive the cipher combination.
- c. Type of container(s) used to store data. Special containers behind locked doors with restricted access are not required. The dot Mil server is password protected. The necessary system administrators and HSA JCSG staff have access to the server. There is intrusion detection at the WHS Backbone level and WHS System Administrators perform periodic log reviews to determine authorized and unauthorized access to the network. The H, S drives and e-mail are backed-up on a daily basis and kept in suite 402 for 90 days. Every Sunday IT staff takes a snapshot of the H, S drives and e-mail and stores that snapshot off-site. That is kept for 1 year at First Federal in Maryland. First Federal is under contract to WHS and much of the Federal Government to store their back-up data.

4. Document Control.

- a. All deliberative documents produced by or submitted to the HSA JCSG (e.g., meeting minutes, information dealing with scenarios, possible alternatives, or recommendation candidates) will be assigned sequential control numbers by the HSA JCSG administrative staff. HSA JCSG

Administrative staff will maintain a document log containing the control number, copy number (copy 1 of N copies if applicable), title and type of document, subject, date, who accessed the data, when data was accessed, and when data was returned.

- b. Access to deliberative or draft deliberative documents and other materials will be restricted, on a need to know basis, to those individuals who have signed non-disclosure agreements that are on file with HSA JCSG or the OSD BRAC office. Deliberative documents will be treated as CLOSE HOLD and maintained in the HSA JCSG secure office space. Authorized individuals who must remove a document or other materials, either electronic or paper copy, from HSA JCSG secure office space must first seek permission from the Chair or Deputy Chair and log out the material on the document control log maintained by the HSA JCSG administrative staff. Minutes of deliberative meetings, information dealing with scenarios, possible alternatives, or recommendation candidates may not be removed from the HSA JCSG secure office. At no time will an employee remove BRAC related data from the HSA JCSG secure office to work at home (this includes e-mail, CD, diskette, or hard copy).
- c. The following is a quote from Policy Memorandum One, referenced above. “To protect the integrity of the BRAC 2005 process, all files, data and materials relating to that process are deemed deliberative and internal to DOD. All requests for release of BRAC 2005 data and materials, including those under the Freedom of Information Act, received prior to the Secretary forwarding his realignment and closure recommendations to the Commission shall be forwarded to the DUSD(I&E).”
- d. Everyone involved in the BRAC 2005 effort must use every precaution to prevent the improper release of, or access to, BRAC 2005 information. Not only is access restricted to those individuals officially approved to take part in the BRAC 2005 process, care must also be taken to avoid inadvertent dissemination of such information through verbal conversation, facsimile, e-mail, or other electronic communication means.

5. **Facsimile.**

The use of facsimile machines to transmit information dealing with scenarios, possible alternatives, or recommendation candidates is not permitted. Information not dealing with scenarios, possible alternatives, or recommendations may be faxed to authorized recipients. Care will be taken to ensure that the facsimile machine is monitored **during transmission and receipt** to preclude any compromise of sensitive information. A sign will be posted on the facsimile machine stating the requirement for monitoring transmissions. The individual sending the facsimile must first call the recipient to ensure that transmission will be monitored by the recipient. After transmission, the sender must call and confirm receipt of the facsimile.

6. Minutes.

The HSA JCSG members will make all deliberative decisions at the HSA JCSG deliberative meetings, not at the subgroup level. The HSA JCSG members' deputies are the designated alternates for the members and have voting authority in the members' absence. Minutes for all JCSG deliberative sessions will be signed by the Chairman of the HSA JCSG and maintained in a secure office space. Minutes of subgroup or team meetings are not required. If minutes are taken for subgroup or team meetings, the original will be maintained in the secure office space. HSA JCSG minutes will record attendance, date/time/location of the meeting, a high-level synopsis of the topics discussed, unresolved issues, and all decisions and recommendations. A literal transcript of the meeting is not required. The OSD BRAC office will also maintain a copy of these minutes.

7. Open Source Data.

Open source data published in regulations, standards, orders, and so on that are produced to control the administration and efficient operation of the Services is deemed reasonable for use in the BRAC process. Open source information does not need to be controlled.

8. Public Affairs Guidance (PAG).

- a. This guidance supplements the OSD PAG dated 13 February 2003, subject: Public Affairs Guidance (PAG) – Transformation Through Base Realignment and Closure (BRAC 2005). Chairs of the HSA JCSG subgroups will forward all press inquiries without comment to OSD Public Affairs, Glenn Flood, 703-697-5131.
- b. Forward all public inquiries to OSD BRAC Office, 703-614-5356.
- c. The HSA JCSG Deputy will forward Congressional inquiries to OSD Legislative Affairs for response.

9. Use of E-mail.

Use of e-mail is permitted from a dot Mil to a dot Mil server for question development, reviewing draft minutes, and other information that does not deal with scenarios, possible alternatives or recommendation candidates. However, use of e-mail to transmit information that does deal with scenarios, possible alternatives or recommendation candidates is prohibited unless the e-mail is sent within the HSA JCSG 1401 Wilson Boulevard location server. It is also prohibited to e-mail any BRAC related information to a dot Com e-mail address (such as a home e-mail address).

10. Analysis.

- a. The joint analytical team supporting the HSA JCSG will strive to conduct all analyses in the HSA JCSG Federal Government office space provided. However, there are situations where software licensing agreements and equipment issues will prevent this from happening. Examples are use of cartographic, simulation, and optimization software or the JCSG's lack of computing hardware. In these instances, electronic copies of data and paper copies of supporting documents will be hand carried to the analyst's parent organization, e.g., CAA, CNA, or AFSAA. The temporary removal of these items will be approved by the Chair or Deputy Chair as outlined in section 4 of this SOP. Once at the parent organization, the security of the sensitive items will meet the same requirements detailed in this SOP.
- b. Specified HSA JCSG staff will perform the analysis.
- c. Technical experts may be used to support the development and/or the refinement of the analytical efforts of the JCSG. The Military Departments and Defense Agencies will identify such technical experts to the JCSG. Each individual will be briefed on the sensitivity of BRAC data, and required to sign a non-disclosure statement. HSA JCSG will maintain a list of individuals authorized to access its data. When technical experts provide information, expertise or data that HSA JCSG considers relevant and appropriate for analyses, the experts shall be requested to submit that information or data in writing with the required certification. Technical experts will be granted only limited access to BRAC 2005 data and information that will allow them to assist the JCSG in the development and/or refinement of analytical efforts. The use of technical experts will be communicated, either orally or in writing, to the ISG.
- d. Analysis will be documented in a sufficient manner to provide adequate audit trails.

11. Office Security.

- a. The HSA JCSG office space is secure and the doors must remain closed and locked at all times. All individuals are responsible to ensure each evening before leaving that their desks are cleared of deliberative papers, their trash receptacles contain no BRAC papers, their office windows are closed and locked, and that they are logged off their PCs.
- b. Visitors (all non full-time employees) must be escorted at all times. BRAC information will be provided on a need to know basis only. Signing a non-disclosure agreement does not guarantee access to all BRAC 05 information. Stop and question strangers and report suspicious activity immediately.
- c. A security checklist though initially considered as necessary, has not been used. Maintenance of such a checklist proved to be cumbersome and elusive. Individuals were responsible to ensure the office space occupied met security standards.

12. Office Procedures for Correspondence.

- a. Official correspondence containing deliberative/certified data will be assigned a controlled document number, which may be obtained from the Office Manager.
- b. All correspondence will contain the following information in the header or footer:

Draft Deliberative Document – For Discussion Purposes Only

Do Not Release Under FOIA

Or

Deliberative Document – For Discussion Purposes Only

Do Not Release Under FOIA

The header or footer will also contain the version number and date that will be updated each time the document is updated as directed by the Deputy, HSA JCSG.

13. Computer Security.

- a. Server log-on passwords must be changed every 90 days. Passwords must contain at least 8 characters, one special character, one number and one capital letter. Passwords may not be reused for at least 10 times. Passwords should not be written down or shared with anyone. Do not allow others to use your login ID or password.
- b. All employees must restart their computers each night before leaving for the day. Restart logs the user off and guarantees that no applications are running in the background. PCs must never be shut down because IT personnel administer patches and update anti-virus software at night. Computers must be locked every time an employee leaves his/her area.
 - (1) To lock: Hold down the Ctrl and Alt keys and press the Delete key, then click on “Lock” in the pop-up dialog box.
 - (2) To unlock: Hold down the Ctrl and Alt keys while pressing the Delete key, then log on by entering your password and pressing the Enter key.

14. HSA JCSG BRAC Certified Database.

- a. Data received from OSD or Services will be received and stored IAW this SOP’s Storage Requirement and Document Control paragraphs. This process is designed to maintain the integrity of the BRAC data. Procedures described herein are utilized throughout the receipt, storage and productive use of the information. The control measures and processes providing this assurance are:
 - (1) Formation of a Data Management Team (DMT) and establishment of operational procedures.
 - (2) Database structure and separation.

- (3) User access controls.
 - (4) Data integrity change tracking logs.
 - (5) Data reconciliation.
- b. Much of the certified data used by the HSA JCSG has not been received through the OSD databases. Due to the various tools used by the responders, and time constraints, a significant portion of the data was received through alternate means. In these cases, every attempt has been made to insure that the data has the necessary documentation for certification. These data and their accompanying certifications (where required) will be cataloged by HSA JCSG to allow easy reference to the data used in our analyses.

15. Formation of the DMT and establishment of operational procedures.

The DMT will consist of the following members:

- a. Military representative. The DMT military representative is the database owner with responsibility for access control permissions, and government oversight.
- b. DMT manager. The DMT manager provides team leadership, task priority management, and execution oversight.
- c. Database administrator. The DMT database administrator maintains direct control of the Master database and operational control over the Production and Test databases.
- d. Programmers/analysts. DMT programmers provide database programming, support and expertise to the HSA JCSG sub-groups.
- e. Technical representative (Tech Rep). Each HSA JCSG subgroup will have at least one Tech Rep. This Tech Rep is the subgroup's liaison between the DMT and their specific subgroup Subject Matter Experts (SMEs). Each Tech Rep will maintain an enhanced understanding of the database and *MS Access*. They will be trained and have working knowledge of certification procedures, and provide quality assurance to ensure integrity of the Production database.

16. Database structure and separation.

The primary architecture of the data environment will be the separation of data into three distinct and segregated databases. These are the Master, Production and Test databases.

- a. Master database. The Master database folder will contain the unmodified OSD or Service original source data. No production or operational work will be performed on this database.

- (1) All original OSD database elements and subsequent OSD updates will be stored as originally received. Each OSD update file will be delivered by either OSD Portal, OSD network transfer area or CD-ROM and will be stored IAW the Document Control procedures in paragraph 4 of this document and Policy Memorandum One. Each file will be maintained on the network in the Master database area as an unmerged original data source. The OSD Portal, OSD network transfer area or the CD-ROMs will serve as an offline backup. The Master database original source files will also be backed up by the network administrator on a weekly basis.
 - (2) The Master database will also contain an integrated updated copy of the database source files. The integrated database created by combining the current files into a single database will be copied to create the Production database.
 - (3) Network rights for “read, write, save” access to the Master database will be restricted to the Military Representative, DMT manager, and Database administrator. No access to the Master Database will be granted to Tech Reps.
 - (4) Information from the Defense Agencies and the DoD activities being reported via OSD.
 - (a) MS Word document input will be converted as stated in the Transformation of MS Word document format data procedures. A copy of the original Word document, the transformed MS Excel spreadsheets and the resultant MS Access files will be stored in their original format before being integrated into the Master database. The DoDIG will be notified when Transformation of MS Word document format data processes are complete.
 - (b) Electronic or database files will be forwarded via OSD Portal, OSD network transfer or CD-ROM.
- b. Production Database. The Production database will contain certified OSD or Service data provided and updated from the Master database and will be the working environment for the DMT and designated Tech Reps from each HSA JCSG subgroup. All queries, reports, and extracts will be taken from this database. Information from this database will be available to HSA JCSG subgroups via Tech Reps. Access to the Production database will be provided to the supporting HSA JCSG Analysis Team. The Production database original source files will be backed up by the network administrator on a weekly basis.

- c. Test database. The Test databases will use certified data but this data is not intended to be maintained in a certified state. This data is intended for testing queries and reports only. These files are not archived and may be deleted when no longer required. They are not used for analysis purposes. No backups are required. Test databases are backed up in the normal network backups but this is not required.

17. **User Access Controls.**

User access control will be maintained at two levels.

- a. Network access permissions insure only those authorized have access to the network.
- b. Folder permissions will limit access within the HSA JCSG environment to designated individuals. Folder permissions are specifically set for each database as required. These specific permissions maintain the sanctity of the Master database.

18. **Data Integrity with OSD and Service Databases.**

The “true replica” state of the original certified Service database information is protected by transmission through the OSD database or via direct transfer from the Service POCs via designated portals or CD-ROM. An update document will include the genealogy and/or data-table updates from OSD and will be provided by OSD in conjunction with the Master database transfer. Whenever changes are received from OSD, the Master database and the Production database will be updated by the database administrator.

19. **Data Reconciliation.**

The ‘true replica’ nature of the Production database is maintained by reconciling the protected Master database and the operational Production database. This is managed by the Database Manager. These audits and checks fall into three categories.

- a. Database update controls. Updating the Master and the Production database will be restricted to the database administrator. The DMT manager will provide oversight of the Master database updates
- b. Non-automated data that has been converted from *MS Word* to *MS Access* will be examined by the respective organization’s designee and the DMT during conversion and prior to integration to the Master database. The transformed data will be checked and audited by the designee and the DMT members that performed the conversion. This process check will be performed on an item-by-item basis during the conversion. A post transformational check of 20 percent of the data will also be made after the data has been recorded before the data is integrated into the databases. DoDIG transformational checks will be performed comparing the original OSD data and the Master database.
- c. The HSA JCSG will perform weekly or as provided downloads and reconciliation checks at various levels:
 - (1) Database to database level file size comparisons.

- (2) Selected table-to-table comparisons.
 - (3) Focused selected record-by-record checks will be performed on actively changing data as required. These reconciliations are performed by the DMT members, by subgroup Tech Reps or subject matter experts. on a spot check and event-driven basis.
 - d. Event-driven checks will be performed by the DMT after abnormal events such as user personal computer system crashes, application lockups or when data appears to be abnormal or corrupted. Data-tables that were being accessed at the time of an abnormal event will be examined and compared to the Master database or reloaded from the source database or file.
20. **Actions to be taken on discovery of data inconsistencies.**
- a. Errors discovered in the merged data sources will be forwarded to OSD, the cause analyzed and the merger process re-accomplished from original data files. Crosschecks will be performed again once merger is complete.
 - b. Errors found in original source files will be forwarded to OSD or the Services by the current data clarification process and documented internally IAW OSD procedures. The OSD or Service corrective action will be documented, and replacement files posted to the OSD Master database. The update files will be downloaded from the OSD Master database. All checks and documentation will be accomplished as in the procedure for original data.
21. **Backups**
- a. Network backups. All network backups will be accomplished by the support IT activity staff on the established recurring basis. All normal procedures will be followed for safeguarding the backup information according to existing support organizational rules. The Master and Production databases will be backed up by the network administrator on a weekly or more frequent basis.
 - b. CD-ROM or equivalent media backups. Record copies of BRAC transformation data and appropriate documents will be created after the completion of Candidate Recommendation process. These disks will be provided to the HSA JCSG Office Manager for permanent retention.
 - c. When we moved into this space, WHS did not back-up anything on the server (no process in place). Now, WHS IT has two types of back up in place. The H and S drives and e-mail are backed-up on a daily basis and kept in suite 402 for 90 days. Every Sunday IT staff takes a snapshot of the H and S drives and e-mail and stores that snapshot off-site. That is kept for 1 year at First Federal in Maryland. First Federal is under contract to WHS and much of the Federal Government to store their back-up data.

22. Data Certification

Listed reference states that DoD Components and JCSGs will establish procedures and designate personnel to certify the data and information collected for use in analyses are accurate and complete to the best of that person's knowledge and belief, and that these procedures will be incorporated into the organization's Internal Control Plan. Procedures governing the HSA JCSG's certification and documentation processes, to include use of certified data, follow:

- a. **General.** Data and information certified by the Military Departments (MILDEP), OSD, the Joint Staff, Defense Agencies and Defense Field Activities as complete to the best of their knowledge and belief will typically be used in all analyses. OSD, or the HSA JCSG Chair, will provide approval and/or certification for use of authoritative sources/databases as information sources.
- b. **Substituting Judgment-Based Data for Certified Data.** Because of the unique nature, breadth, and scope of the analysis of this JCSG, there will be cases where despite best efforts certified data will not be obtainable. Data is required in every field of all military value scoring plans. Models will not run with missing data. In cases where data does not exist for a particular field, or is otherwise unobtainable, judgment-based data will be used to fill the missing data. The judgment-based data will be constructed by functional subject matter experts in consultation with MILDEP and 4th Estate liaison representatives. Every attempt will be made to make the judgment-based data a fair representation, providing no intentional benefit or detriment to the entity that is missing data. Each case of judgment-based data will be explicitly addressed and approved by the JCSG Members before its implementation. In any case, certified data will supersede any judgment-based data; all attempts will be made to find appropriately certified data. Use of judgment-based data will be documented in the minutes of the JCSG deliberative sessions.
- c. **Judgment-Based Assumptions.** From time-to-time, the JCSG will need to use judgment-based assumptions as the basis for analyses. An example is the percentage of personnel reduced as a result of a joint service consolidation. Certification is a concept that applies only to factual information, therefore methodologies leading to judgment, the methodology to arrive at that judgment, and associated assumptions cannot be certified. As in b. above, the record will reflect what judgment was used and why, or what assumptions underlay the analysis. Minutes that explain the basis for an assumption or judgment, or other record, will document the decision.



Donald C. Tison
Assistant Deputy Chief of Staff, G-8
Chairman, HSA JCSG