Non disclosure
Val Jurneau

**Standard Operating Procedures for the
Medical Joint Cross-Service Group (MJCSG)
Base Realignment and Closure 2005**

1. PURPOSE.

This document contains important information on standard operating procedures related to controls necessary to safeguard the BRAC 2005 deliberative data, documents, decisions, and recommendations for the MJCSG. All individuals working within the BRAC 2005 process or providing support to the process will be required to sign a non-disclosure agreement.

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.*

Send to Mayor

3. STORAGE REQUIREMENTS.

a. Physical location used to store data. All BRAC 2005 data will be securely stored at the MJCSG Federal Government office space at 1401 Wilson Boulevard, Suite 400, Arlington, Virginia 22209.

b. Physical security for the location. The entrance to the office space is secured by a cipher lock on the front and back door. The Security Manager will change the cipher lock combinations every three months or in the event, an employee leaves the organization. The MJCSG staff will receive the cipher combination. A log will be kept to record when the cipher locks were changed and who changed them.

All deliberative data will be locked in a cyber-lock safe is located in the central MJCSG office behind a locked door. The central office is located within a centrally secure office complex behind a main cyber-locked entrance. The dot mil server is password protected. The necessary system administrators and MJCSG staff have access to the server. There is intrusion detection at the WHS Backbone level and System Administrators perform periodic log reviews to determine authorized and unauthorized access to the network. Electronic, deliberative information such as analysis questions; will be backed up daily by an on-site network administrator.

4. DOCUMENT CONTROL.

a. All deliberative documents produced by or submitted to the MJCSG (e.g., meeting minutes, information dealing with military value scoring plans and weights, scenarios, possible alternatives, or recommendation candidates) will be assigned sequential control numbers by the MJCSG administrative staff. Medical JCSG members will work with a copy of the original data

call data. MJCSG 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, signature of who accessed the data, where and when returned.

b. Access to deliberative or draft deliberative documents and other materials will be restricted to those individuals who have signed non-disclosure agreements that are on file with MJCSG or the OSD BRAC office. Deliberative documents will be treated as CLOSE HOLD and maintained in the MJCSG secure office space. Authorized individuals who must remove a document or other materials, either electronic or paper copy, from MJCSG secure office space must first obtain written permission from the Chair or MJCSG ~~Secretary~~ DOC and sign for the material on a sign-out log maintained by the MJCSG administrative staff. Minutes of deliberative meetings, information dealing with scenarios, possible alternatives, or recommendation candidates may not be removed from the MJCSG secure office.

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. MJCSG DATA MANAGEMENT PROCEDURES.

The MJCSG BRAC certified database data received from OSD will be marked, 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:

a. Formation of a Data Management Team (DMT) and establishment of operational procedures.

b. Database structure and separation.

c. User access controls.

d. Data integrity change tracking logs.

e. Data reconciliation.

"SOPs will be reviewed on a regular basis to ensure individuals are following the guidelines and changes are made based upon additional/revised guidance provided by the OSD BRAC office and additional procedures that may be required."

6. FORMATION OF THE DMT AND ESTABLISHMENT OF OPERATIONAL PROCEDURES.

The DMT will consist of the following members:

- Military Representatives (Lt Col Lei Jones) ~~Major~~ Major Michaelle Guerrero
- DMT Managers (CDR Nancy Hight, Major Michaelle Guerrero, ~~Major Doug Harper~~) Mr Brian Barton - Lt Col Lei Jones 16Jan04 WM 16Jan 04
- Database Administrators (Mr. Bob Opsut, Mr. Dan Curry, CDR Nancy Hight, Major Michaelle Guerrero,)
- Analysts (Mr. Joseph Fanzone, Mr. Brian Barton, CDR Judith Bellas, Major Cook) CDR James Bradley, HM1 Anna Deco

DMT Military Representative: The DMT Military Representative is the database owner with responsibility for access control permissions, and government oversight.

DMT Managers: The DMT Managers provide team leadership, task priority management, and execution oversight.

DMT Database Administrators: The DMT Database Administrators maintain direct control of the Master Database and operational control over the Production and Test databases. The Database Administrators 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.

It is the responsibility of the DMT to ensure that each subgroup's database and informational needs are met. Each subgroup will work through their respective Database Administrator to coordinate with the DMT.

DMT Analysts: The DMT Analysts provide database programming, support and expertise to the MJCSG subgroups. Each MJCSG subgroup will have at least one Database Administrator.

7. DATABASE STRUCTURE AND SEPERATION.

The primary architecture of the data environment will be the separation of data into 3 distinct and segregated databases.

a. Master database. The Master database will contain both the unmodified original source files and the consolidated (merged) data. The consolidated

data will be maintained separately. No production or operational work will be performed on this database.

(1) All original OSD database elements and subsequent OSD updates will be stored in originally received files. Each OSD update file will be delivered by CD-ROM* and these CD-ROMs will be documented and 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 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 daily basis.

* or ftp (file transfer protocol), or lan (local area network)

(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) Access to this database will be restricted to the Military Representative and DMT Managers.

(4) The integrated Master Database will be backed up by the network administrator on a daily basis.

b. Production database. The Production Database will contain certified data provided and updated from the Master Database and will be the working environment for the DMT from each MJCSG subgroup. All queries, reports, and extracts will be taken from this database. Information from this database will be available to MJCSG subgroups. Access to the Production Database will be provided to the supporting MJCSG Analyses Team.

Two concepts will be used to keep Analyst data current. The first concept is a version control reference hypertext document that will provide information on the current changes and data version dates. The information is broken down into changes catalogued by specific date and separately though a listing sorted by question number indicating the current table version date.

Secondly, the source OSD response tables will be date tagged at record level by the proponent Service. This 'record level' suffix indicates the date of the information record. These fields will be passed down from OSD integrated into the data record. Analyst level reports can now contain both a print date and an information 'as of' date.

The Production database original source files will be backed up by the network administrator on a daily basis.

c. Test database. The test database allows for the safe creation and evaluation of forms, queries and reports by the DMT analysts. Once created, these user interfaces are tested to ensure that they do not have undesirable impacts.

(1) The testing criteria are:

A. Data is not modified by the user query or report.

B. **Queries and forms produce the intended results.**

(2) The following restrictions are in place for this database area:

A. At inception, the Test Database will be populated with certified data but this data is not intended to be maintained in a certified state. The data may be customized during the testing process creating modified or abnormal data.

B. Access permissions are restricted to DMT team members only. Access control is accomplished using user permission, rights and network privileges. **User access controls.** User access control will be maintained at three levels.

d. Network access permissions ensure only those authorized have access to the network.

e. Folder permissions will limit access within the MJCSG environment to designated individuals on the DMT, and Analysis Team. Folder permissions are specifically set for each database. These specific permissions maintain the sanctity of the Master Database and the isolation of the Test database.

f. In the Production database, *MS Access* database level permissions are designed to restrict access to each database by authorized individuals.

8. DATA INTEGRITY CHANGE TRACKING LOGS.

The "true replica" state of the original certified Service database information is protected by recording its history. A posting log will include the genealogy and chain of custody of database or data-table updates from OSD into the Master Database. Whenever changes are received from OSD to the Master Database, the Production Database will be updated by the Database Administrator and these changes cross-checked by the DMT Manager. With this cross-check in place, data can be compared, validated, and synchronized while maintaining the 'true replica' nature of the Production Database.

9. 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 Databases will be restricted to the database administrator. The DMT manager will cross check 100 percent of the Master database updates.

b. Reconciliations: Reconciliations are performed by the DMT, subgroup analysts and SMEs. The JCSG will perform monthly reconciliation checks at various levels:

Production Database

- A copy of the Master Database is placed on a CD and in a local drive on each Analyst's machine. This database is left in Read-Only status to ensure data integrity.
- Each Analyst has a working copy of a database that uses an incorruptible link to the Read-Only copy of the Master Database.
- Each Wednesday (or when available) the latest version of the Master Database will replace the previous version on each Analyst's machine and the incorruptible link will be refreshed. This will ensure the most current version is used.
- Each Wednesday (or when available) a Change Report will be generated indicating which values were added/changed/deleted.
- A log is kept, showing the Database Name and date created. The name and date will be used to validate that the Analyst is using the correct version and that the Read-Only status is in tact.
- The Master Database CD is labeled and kept secure in Cyber Lock safe.

16 June 04

Mr. Brian Barton
Database Manager
MJCSG
16 June, 2004

(1) Database-to-database level global comparisons.

(2) Selected table-to-table comparisons.

(3) Focused selected record-by-record checks will be performed on 20 percent of the actively changing data areas. Priority will be given to data that has been accessed repeatedly since the last reconciliation check. Lower priority will be given to data that has not been actively accessed since the last reconciliation.

(4) SMEs will provide "quick look" spot checks on a monthly and event-driven basis.

c. Event-driven checks: Event-driven checks will be performed by the DMT after abnormal events such as user personal computer system crashes, software 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.

d. Data Quality Assurance: Data Quality Assurance (QA), Quality Control (QC) and Data Certification. The Database Implementation Plan addresses the QA, QC and Data Certification plan in expanded detail. These three concepts work together ensuring that the database remains certifiable and viable for information analysis. The process is:

(1) QA: Software QA involves the entire software development PROCESS - monitoring and improving the process, making sure that any agreed upon standards and procedures are followed, and ensuring that problems are found and dealt with. It is oriented to 'prevention'.

(2) QC: QC is a process for maintaining standards and not for creating them. QC measures both data and processes for conformance to quality requirements MJCSG will do statistical sampling checks on the *MS Word* to *MS Access* transformational data.

10. DATA CERTIFICATION.

The DoD IG will do statistical QC as a managerial process during which actual process performance is evaluated and actions are taken on unusual performance. It is a process to ensure the data maintains its original value and the certification. Certification is ensuring the "chain of custody" of data is maintained from originator to analyst.

11. ACTIONS TO BE TAKEN ON DISCOVERY OF DATA INCONSISTENCIES.

a. Errors generated in the merging of data sources: Errors generated in the merging of data sources will be documented, the cause analyzed and the merger process re-accomplished from original data files. Cross-checks will be performed again once merger is complete.

b. Errors found in original source files: Errors found in original source files will be forwarded to the OSD DST and documented internally and IAW OSD procedures. The OSD corrective action will be documented, updated files archived, and replacement files posted to the Master Database. The files will be integrated into the Master Database. All checks and documentation will be accomplished as in the procedure for original data.

12. BACKUPS.

a. Network backups: All network backups will be accomplished by the support OSD IT 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, Production and Test databases will be backed up by the network administrator (CNA) on a daily basis.

~~b. CD-ROM back ups: All OSD source CD-ROMS an~~ Hgmes, LtCol

13. DATA STORAGE.

Space will be allocated within the cyber-safe for MJCSG workgroups to have their own file storage system. BRAC data/information needing to be secured during or after duty hours will be stored in the cyber-safe. A document log will be kept in the safe to annotate the movement of documents, (title and type of document which includes data whether disk or paper format, subject, date, signature of who accessed the data, when returned.) The Medical Joint Cross Service Group will always maintain a master copy of the data provided for its analyses. To ensure that data is not modified as it gets entered into analytical tool/systems, or passes from one tool/system to the next; a series of random master data runs will occur. The outcome of the data runs will encourage comparison of documents to the original source.

14. 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 a trusted agent monitors the facsimile machines 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.

15. MINUTES.

The MJCSG members will make all deliberative decisions at the MJCSG deliberative meetings, not at the subgroup level. Minutes for all MJCSG deliberative sessions will be signed by the Chair of the MJCSG. Meeting minutes will be 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. MJCSG 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.

16. 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. However, base realignment and closure recommendations will be based solely on information that is certified as accurate and complete to the best of the certifier's knowledge and belief. Open source information used to support MJCSG analyses will be filed in the same facility as other data. The use of open source data in the MJCSG analysis is protected information; the source and details of the data used will be afforded the same protections as all other data.

17. 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 MJCSG subgroups will take all press, public, or Congressional inquiries without comment and forward with proposed answers to the MJCSG Secretary. Forwarded inquiries should include the publication name, reporter's name, and deadline.

b. In the event of a public inquiry, the recipient should determine the questioner's name, contact information and if the inquiry is on behalf of an organization. If applicable, obtain the name of the organization the questioner represents.

c. The MJCSG Secretary will forward Congressional inquiries to OSD Legislative Affairs for response.

18. USE OF EMAIL.

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. MJ~~CSG data analysts will not have access.~~

to email or Internet on their computers. A separate computer with email and Internet access will be available for their use.

19. PERFORMING ANALYSIS.

a. Analysis of certified data, scenarios, etc. must be conducted at the MJCSG secure office space.

b. A list of MJCSG staff will be maintained by the MJCSG Secretary.

c. Specified MJCSG staff will perform the analysis.

20. OFFICE SECURITY.

a. The MJCSG office space is secure and the doors must remain closed and locked at all times. A security check will be conducted daily and a security checklist will be filled out by the last person to leave the office. It is each individual's responsibility 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 of their PCs, and that they have closed and locked their office door.

b. Staff (full-time employees) will not bring personal computers, cell phones or PDAs with video capability into the secure MJCSG office space.

c. Visitors (all non full-time employees) must be escorted at all times and must wear a visitor badge. 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.

d. The data areas will be equipped with computers and conference space. A visitor log will be present at the MJCSG front desk for "sign in", along with visitor identification tags. Visitors must turn PDAs and cell phones **off** while in the secure area. At no time will a visitor be allowed to bring a personal computer into the area.

21. OFFICE PROCEDURES FOR CORRESPONSENCE.

a. All printed material is considered deliberative in nature and must be safeguarded. Official correspondence 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 which will be updated each time the document is updated.

**Data may be copied onto another data vehicle (CD, thumb drive, etc.) and removed from the office with the signature of 2 trusted agents only (the Secretary must be one).

22. PROCEDURES FOR BRAC MJCSG E-ROOM.

a. The E-Room is an Internet Web site available to members of the MJCSG. The site contains a point of contact list, calendar, announcements and shared documents may be posted there. The E-Room is for **Open Source, non-deliberative** information only.

b. The Office Manager will provide individual access to the E-Room. User IDs are lower case first initial and last name.

c. Passwords must be changed the first time a user logs in. To change a password, click on Site Settings, User Information, Edit My Information, and Change Password. Passwords must be different from your network logon password and they must be changed every 90 days. Passwords must contain at least 8 characters, one special character and one capital letter. Passwords may not be reused for at least 10 times. Passwords should not be written down or shared with anyone.

23. 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 will not be written down or shared with anyone.

b. All employees must log-off their computer each night. PCs must be shut down on Friday evenings. They must also be locked every time when the employee leaves their area.

c. To lock: Hold down the Ctrl and Alt keys and press the right Delete key, then click on "Lock" in the pop-up dialog box.

d. To unlock: Hold down the Ctrl and Alt keys while hitting the Delete key, then log on by entering your password and hitting the Enter key.

24. MJCSG RECORD KEEPING.

a. Personnel

Mr. Jack Hoggard– AF OSD Office Liaison

Lt Col Lei Jones – MJCSG POC

b. Signed Nondisclosure Agreements

c. Minutes

d. Data, information, analyses, and descriptions in making recommendations

e. Changes to the Standard Operating Procedure per Secretary MJCSG approval.

GEORGE P. TAYLOR, JR.
Lieutenant General, USAF, MC, CFS
Chair, Medical Joint Cross Service Group