

DCN: 2496

APR 1 2004

STANDARD OPERATING PROCEDURES
FOR
SAFEGUARDING BASE REALIGNMENT AND CLOSURE DATA

References:

1. Memorandum, Secretary of Defense, 15 Nov 02, Subject: Transformation Through Base Realignment and Closure.
2. Memorandum, Secretary of Defense, 13 Feb 03, Subject: Public Affairs Guidance Transformation Through Base Realignment and Closure.
3. Memorandum, Under Secretary of Defense (Acquisition, Technology, and Logistics), 16 Apr 03, Subject: Transformation Through Base Realignment and Closure
4. Policy Memorandum One – Policy, Responsibilities, and Procedures.
5. Appendix B, Office of the Secretary of Defense Internal Control Plan for the 2005 Base Realignment and Closure Process.
6. Standard Operating Procedure for BRAC Office, 1401 Wilson Blvd., Rosslyn, VA.

1. Purpose: To establish standard operating procedures (SOP) for the Professional Development Education (PDE) subgroup of the Education & Training Joint Cross Service Group (JCSG) for safeguarding Base Realignment and Closure (BRAC) data.

2. Background: The Office of the Secretary of Defense Internal Control Plan (ICP) establishes the policies and responsibilities for the protection of data to prevent premature dissemination. It is the responsibility of each JCSG and its respective subgroups to assure internal controls and SOP is in place for handling information received in data calls. The subgroup chair of each designated BRAC group will assure all assigned members of the group have signed non-disclosure statements and are informed that no internal deliberation or data will be discussed or shared with anyone outside their respective groups. The goal is to assure accuracy, completeness, and integration of all information and analytical processes upon which BRAC 05 recommendations are based and to limit the possibility of premature or improper disclosure. This includes inadvertent dissemination of BRAC information through any means.

3. Administrative Requirements:

- a. Storage Requirements: All PDE BRAC working data will be kept in room 1B474A Pentagon, Arlington Virginia or in the E&T JCSG workspace located at 1401 Wilson Boulevard, Rosslyn, VA. These will be the only authorized storage and data analysis work locations. The Pentagon is a badge controlled access building with uniformed guards controlling access to the building. The room (1B474A) is protected by card lock and cipher keypad. The Joint Staff Security Office will change the cipher lock combination, whenever a PDE subgroup member leaves the BRAC team. All members of

**STANDARD OPERATING PROCEDURES (SOP)
FOR ADMINISTRATION AND MANAGEMENT OF THE
JOINT CROSS SERVICE GROUP (JCSG) SPECIALIZED SKILL
TRAINING (SST) PROGRAM TO SAFEGUARD BRAC 2005 DATA**

25 APRIL 2005

1. The Office of Secretary of Defense Internal Control Plan (ICP) establishes the policies and responsibilities for the *Protection of data to prevent premature dissemination*. The Chair of each designated BRAC group will ensure all assigned and substitute members of his or her group are informed that no internal deliberation or data will be discussed or shared with anyone outside their group without specific Chair approval.

2. ADMINISTRATIVE RESPONSIBILITIES

a. E&T JCSG-SST Conference Room: SAF/AQ Conference and Innovation Center, Suite 900, Conference Room 2, 1560 Wilson Blvd, Rosslyn, Virginia, 22209.

b. Personnel responsibilities: The Chair of the E&T JCSG-SST is Brigadier General Gilmary M. Hostage III who is responsible for compliance with the SECDEF ICP and the security of/access to BRAC information related to the E&T JCSG-SST subgroup. The Chair shall designate a Point of Contact (POC) who shall ensure compliance with this instruction. The POC is Col James E. Briggs who is responsible for the subgroup's daily conduct, maintenance of the Non-Disclosure Agreements, and the security of the entrusted sensitive information. The E&T JCSG-SST Suite Custodian is Ms Annette Atoigue who is responsible for the facilities, phones, and office equipment. Additionally, Ms Atoigue maintains a Suite Access Log. E&T JCSG-SST Subgroup members are responsible to secure the Suite 900 common use workstations at the end of each day. E&T JCSG-SST members will be prohibited from bringing outside laptop computers into Conference Room 2. The last individual out of Conference Room 2 shall ensure the computers are off/secured, lights are turned off, the file cabinets are secured, and the door is locked.

c. Storage requirements: Access to the building is controlled by a DATAWATCH Systems card reader, the Suite is protected by an A-Team card reader, and Conference Room 2 secured with a keyed door lock. The Suite Custodian, Ms Annette Atoigue, and the 4th floor security maintain keys to all Conference rooms. Data will be stored in locking file cabinets within Conference Room 2. The POC and CDR Greg Hilscher have keys to Conference Room 2 and the SST common-use locking file cabinet. All team members have access to the common-use file cabinet. Computer security will follow standard DOD computer security requirements. Computers will be password protected and must have password protected screen savers.

d. Control Requirements: The SST Subgroup Chair has designated the Chair, POC, and Deputy POC (CDR Hilscher) as the only individuals with access to the original deliberative documents (e.g., data call responses, information dealing with scenarios, possible alternatives, or recommendations). The original deliberative documents will be stored in a separate locking filing cabinet within Conference Room 2. The SST Subgroup Chair, POC/Deputy POC (plus suite custodian) will be the only individuals with keys to this filing cabinet. Controlled Data (Certified disks) will be inventoried, dated, logged, and assigned a control number when received. The POC/Deputy POC will maintain a Master Data Log. The Subgroup Chair, or POC/Deputy POC must approve copies of controlled data. Additional copies will only be made on a limited basis to support questions, notes, and analysis. The same control number will be used for each copy and annotated with the copy number. The POC/Deputy POC will maintain a sign-in/out log. Copied data will be inventoried, dated, logged in the same fashion as original data. Copies, notes, or computations cannot leave the secure area without approval from the SST Subgroup Chair, POC/Deputy POC. The POC/Deputy POC will maintain a transit log to identify what information left the facility, who took it out, where it was stored, and when it was returned. Subgroup Chair or POC/Deputy POC are authorized to remove original data from the facility. If individuals are authorized to leave the facility with BRAC data, they must have sufficient containers to store the information and have the ability to restrict access to the container. Deliberative documents will be properly marked with the following BRAC headers and footers: Draft Deliberative Document-For Discussion Purposes Only, Do Not Release Under FOIA or Deliberative Document-For Discussion Purposes Only, Do Not Release Under FOIA. Under no circumstances will deliberative documents (including but not limited to scoring plans, computations, scenarios, and recommendations) be emailed.

e. Access Requirements: Data access will be limited to members of the JCSG-SST Subgroup and to those the Chair designates. The POC will provide a list of individuals granted authority to access Conference Room 2 to the SST Subgroup Suite Custodian. The list may be modified only with the approval of the Subgroup Chair or POC. Individuals who are not on the list will not be granted access regardless of grade or rank. The POC will maintain a list of individuals who have signed a Non-Disclosure Agreement. The Subgroup POC will serve as the point of contact for gaining access and scheduling availability of data as required. The SST Subgroup Suite Custodian will maintain an Access Log. Each primary Subgroup member (service designees) will have access to the data. However, the Subgroup POC will make the determination whether varying levels of access are authorized for support members based upon the particular situation. The Chair or POC is authorized to grant one time access to data/secure area for Subject Matter Experts (SMEs). SMEs are not authorized to remove any of the data in any form (hard copy, notes, electronic) from the data storage area. Subgroup POC will ensure all SMEs have signed Non-Disclosure Agreements. All SST approved visitors will sign the Access Log.

f. Document Destruction. As required, BRAC documents will be placed in the Suite locked "Shred-It" bin for disposition. Each SST member is responsible to ensure all BRAC related documents not under document control are placed into the Suite shredder bin.

g. E-Mail Use. E-Mail use 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 Military Value Scoring Plans, data call responses, scenarios, possible alternatives, or Candidate Recommendations. Use of E-mail to transmit information dealing with Military Value Scoring Plans, data call responses, scenarios, possible alternatives, or Candidate Recommendations is prohibited.

h. Other Requirements: All data, including electronic, originals, and copies, will be centrally stored. To prevent unauthorized access to data submissions, Conference Room 2 access will be restricted by locking Conference Room 2 whenever vacant. The POC will run periodic checks (monthly) to ensure only authorized individuals are gaining access to the facility and data, how much information is being copied, how much information is leaving the facility, and whether the data is under positive control. SOP will be reviewed on a monthly basis and updated as required.

3. RECEIPT OF DATA CALL INFORMATION FROM E&T JCSG CHIEFS

a. E&T JCSG Chiefs will provide the E&T JCSG SST subgroup with the BRAC data call information via CD-ROM. The SST POC/Deputy POC/Data Manager are authorized to transport the BRAC information. While transporting BRAC information, media should be appropriately covered with close hold cover sheet and protected from possible disclosure.

b. Upon arrival back at the SST work site, 1560 Wilson Street, Rosslyn, the CD will be logged according to the SST SOP section 2d. The POC will copy the CD onto the SST Conference Room computer using the D Drive, BRAC file. The SST POC will verify everything was copied from the CD to the D Drive, BRAC file. The CD will then be secured in accordance with SST SOP section 2d. This CD will not be used again unless the file on the D Drive should become corrupt. Paper copies of the D drive BRAC information will be logged and distributed to SST members according to SST SOP 2d. The Chair, POC/Deputy POC are the only members of the subgroup who are authorized to make copies of the BRAC information. SST members are required to secure the paper copies of BRAC data according to 2d.

4. TRANSFER OF INFORMATION INTO THE SUBGROUP ANALYSIS TOOL

a. The SST POC designates the SST data manager and Service SST members authority to take the information off the D drive BRAC file and input it directly into the SST analysis tool. Each member is responsible for verifying the accuracy of the BRAC information entered into the tool. SST members who enter BRAC information into the tool must have another SST member verify information accuracy. If data entry errors are discovered, the member committing the error or POC/Deputy POC will make immediate corrections and the change revalidated for accuracy.

5. RECEIPT OF SUPPLEMENTAL DATA CALL INFORMATION FROM E&T JCSG CHIEFS

a. E&T JCSG Chiefs will provide the E&T JCSG SST subgroup with the BRAC supplemental data call information via CD. The SST POC/Deputy POC/Data Manager are designated the individual authorized to transport the BRAC information. While transporting BRAC supplemental information, media should be appropriately covered with close hold cover sheet and protected from possible disclosure.

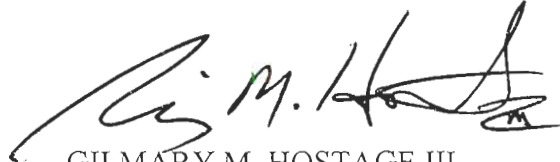
b. Upon arrival back at the SST work site, 1560 Wilson Street, Rosslyn, the CD will be logged according to the SST SOP section 2d. The POC will copy the CD onto the SST Conference Room 2 computer using the D Drive, BRAC file. The supplemental information will be stored in folders on the D Drive, BRAC file as follows:

- a. Data Call Number
 1. Army
 - a. Question 103 (Example)
 - b. Question 108 (Example)
 2. Navy/Marine Corps
 3. Air Force
 4. Defense Agencies

The SST POC will verify everything was copied from the CD to the D Drive, BRAC file. The CD will then be secured in accordance with SST SOP section 2d. This CD will not be used again unless the file on the D Drive should become corrupt. Paper copies of the D drive BRAC Supplemental information will be logged and distributed to SST members according to SST SOP 2d. The Chair and POC/Deputy POC are the only members of the subgroup who are authorized to make copies of the BRAC Supplemental information. SST members are required to secure the paper copies of BRAC supplemental data according to 2d.

c. The SST POC/Deputy/Data Manager are responsible for incorporating supplemental data into the D Drive BRAC files. The SST POC/Deputy/Data Manager will identify the specific question, data element, and response to be changed. In the electronic files (MS Access and MS Word), the SST POC/Deputy/Data Manager will key enter updated response in the appropriate location(s) and in the MS Word add a footnote that includes the date, log number and change. For PDF files, the SST POC/Deputy/Data Manager will attach a comment (date, log number and change) to the specific PDF file that is being updated. A Service SST member will verify the supplemental data was updated correctly into the D Drive BRAC files. If data entry errors are discovered, the POC/Deputy/Data Manager will make immediate corrections and the change revalidated for accuracy. The POC/Deputy/Data manager will identify to the Service SST members that supplemental data has been received and changes are required in the data tool.

d. The SST POC authorizes the SST data manager and Service SST members to take the information off the D drive BRAC supplemental file and input it directly into the SST analysis tool. Each member is responsible for verifying the accuracy of the BRAC supplemental information entered into the tool. SST members who enter BRAC supplemental information into the tool must have another SST member verify information accuracy. If data entry errors are discovered, the member committing the error or POC/Deputy/Data Manager will make immediate corrections and the change revalidated for accuracy. The SST data manager and Service SST members must review all analysis tools to determine all areas impacted by the supplemental information.



GILMARY M. HOSTAGE III,
Brigadier General, USAF
JCSG-SST Chair

E&TJCSGFTSG Notice 5000/
01 April 2005

**STANDARD OPERATING PROCEDURE (SOP) FOR INFORMATION
SECURITY WITHIN THE EDUCATION AND TRAINING (E&T) JOINT
CROSS SERVICE GROUP (JCSG), FLIGHT TRAINING SUBGROUP FOR
THE BASE REALIGNMENT AND CLOSURE (BRAC) COMMISSION 2005**

1. PURPOSE

This document contains important information on the Standing Operating Procedures (SOP) related to controls necessary to safeguard the BRAC 2005 deliberative data, documents, decisions, and recommendations for the E&T JCSG Flight Training Subgroup.

2. DIRECTION

The office of the Secretary of Defense (SECDEF) Internal Control Plan (ICP) establishes the policies and responsibilities for the protection of sensitive data to prevent its premature dissemination or disclosure. The Chair will ensure all assigned and substitute members of his or her group are informed that no internal deliberation or data will be discussed or shared with anyone outside their group without specific Chair approval.

3. KEY POINTS OF CONTACT/ADMINISTRATIVE RESPONSIBILITIES

- a. The Chair of the E&T, JCSG, Flight Training subgroup is: RADM George Mayer. He is responsible for compliance with the SECDEF ICP and the security of/access to BRAC information related to the E&T, JCSG, Flight Training subgroup. The Chair shall designate a Point of Contact that shall ensure compliance with this instruction and instructions promulgated by higher authority.
- b. The E&T, JCSG, Flight Training subgroup Point of Contact is: CAPT Gene Summerlin, USN. Responsible for the subgroup's daily conduct, maintenance of the Non-disclosure Agreements and Facility Access Logs and the security of the entrusted sensitive information.
- c. The E&T, JCSG, Flight Training subgroup Team Leader is: Col Jimmie Simmons, USAF. Responsible for the daily execution of tasking and tactical Team direction.
- d. The E&T, JCSG, Flight Training subgroup Assistant Team Leader is: Lt Col Gary Wolfe.

Draft Deliberative Documents – For Discussion purposes only
Do not release under FOIA.

- e. The E&T, JCSG, Flight Training subgroup Room Custodian is: CDR John Lund. Responsible for the facilities, phones, office equipment, to provide key control to Room 3052. The Room Custodian shall maintain a log of those members that have been issued keys.

4. STORAGE / SECURITY / ACCESS REQUIRMENT

- a. Physical location used to store data. All BRAC 2005 data will be securely stored at the E&T, JCSG, Flight Training subgroup Federal Government office space at the Navy Annex, Room 3052.
- b. Physical security for the location. A computer key lock on the main door secures the entrance to the office space; all other access doors are secured and blocked. All individuals without a key are required to utilize the Visitor Register log (located at the doorway for Room 3052). A Key Log is maintained identifying who has access to Room 3052.
 - i. Physical Access. Individuals receiving access to Room 3052 must be part of BRAC 05 and have a need to know E&T JCSG BRAC information. First time individuals must be escorted by subgroup POC's and are required to provide a signed Non-disclosure Agreement to the subgroup Security Manager. Any individuals present that are not on the subgroup Phone Roster will not be granted access. Last person out of the office for the day shall complete the Secured Office Checklist
- c. Hard copy storage. Special containers to store hard copy files are not required within Room 3052 since the room is secured behind locked or blocked doors, which limits access to authorized personnel. However, subgroup staff members will ensure their documents are properly protected, safeguarded, and stored in locked file when not in use.

5. DOCUMENT CONTROL

- a. Transportation of Information. Subgroup members are the only individual authorized to transport original documents, computer disks, etc. Documents must be concealed and have "CLOSE HOLD" denoted on the outer covering.
- b. Preserving documents. All master files and documents shall be maintained in an electronic (normally .PDF) or paper format. When required for reference material, for the Subgroup Office, paper copies may be maintained at the discretion of the Staff Member.

Draft Deliberative Documents – For Discussion purposes only
Do not release under FOIA

Draft Deliberative Documents – For Discussion purposes only
Do not release under FOIA

- c. Copies of Information. All copies made for in-house purposes will be collected same day by a staff member and destroyed weekly through a local shredding center.
- d. Information Access. Access to copies of deliberative and/or draft deliberative documents will be restricted to those individuals who have signed Non-disclosure Agreements that are on file in Room 3052 and on a need to know basis. All deliberative documents are "CLOSE HOLD" information and shall be maintained in the subgroups secure office space. Authorized individuals who remove copies of deliberative and/or draft deliberative documents (electronic or paper) from 3052 must first obtain permission from the subgroup POC or Team Leader and sign for the material in the sign-out log maintained at the Access Door. The following is a quote from Policy Memorandum One from the Under Secretary of Defense (Acquisition, Technology, and Logistics), 16 April 2003.

"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 Defense Base Closure and Realignment Commission shall be forwarded to the Military Department BRAC Authority concerned, or the DUSD (I&E)."

- e. Data Requirements specific to the subgroup. All Request For Clarification (pertaining to Capacity and Military Value) will be entered into an Excel spreadsheet for tracking. A weekly report shall be submitted to OSD (Mr. Howlett) delineating the progress. All data shall be entered into the OSD CAD/MAD databases and have certification to be used in calculating station capacity and Military Value.
- i. Scenario Data Calls (SDC) shall be entered into the OSD tracker for Education and Training number assignment (in Rosslyn). This SDC tracker will be updated weekly following the E&T JCSG meeting.
 - ii. The HSA COBRA Input spreadsheet shall be utilized to input data and build COBRA (.CBR) files.
 - iii. All SDCs shall be stored/transferred via the OSD portal.
- f. Other Requirements. All data, including electronic, originals, and copies, will be centrally stored in Room 3052. To prevent unauthorized access to data, room access will be restricted by controlled access to Room 3052.

Draft Deliberative Documents – For Discussion purposes only
Do not release under FOIA

**Draft Deliberative Documents – For Discussion purposes only
Do not release under FOIA**

- i. A **Master Data Call Binder** shall be established, when necessary. It shall be stored in Room 3052, when not in actual use. The Room Custodian shall incorporate supplemental data call reports into the Master Data Call Binder.
 - ii. No copies shall be made of the information in the Master Data Call Binder without the consent of subgroup Point of Contact. All retrograde information shall be maintained in an additional binder, Retrograde Data Call Binder, logged and stored in Room 3052.
 - iii. All data produced by the E&T JCSG Flight Training Subgroup shall be properly labeled with BRAC headers and footers. Candidate Recommendations (Scenarios) must be blessed by the JCSG prior to advancing to the ISG.
- g. **Information Disclosure.** 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.
- h. All team members must lock their workstations when leaving room 3052. Workstations must be shut down on Friday evenings.
- i. **Information Security Breach.** All precautions must be taken to avoid loss/unauthorized release of "CLOSE HOLD" information that is considered or produced by the subgroup. Attention to detail and training are the best preventative measures to avoid a security breach. However, if a security breach incident occurs, follow the procedures set forth in the E&T JCSG SOP.

6. FACSIMILE

The use of facsimile machines to transmit information such as Military Value Scoring Plans, data call questions and responses, scenarios, possible alternative, or recommendation candidates is prohibited.

7. PUBLIC AFFAIRS GUIDANCE (PAG)

- a. The Subgroup Chair will take all press, public, or Congressional

**Draft Deliberative Documents – For Discussion purposes only
Do not release under FOIA**

Draft Deliberative Documents – For Discussion purposes only
Do not release under FOIA

Inquiries without comment and forward with proposed answers to the E&T JCSG Coordination Team. Forwarded inquiries should include the publication name, reporter's name, and deadline.

- b. If the inquiry is from the public, 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 E&T JCSG Coordination Team will forward Congressional Inquiries to OSD Legislative Affairs for response.

8. USE OF E-MAIL

Use of e-mail is permitted from a dot Mil to a dot Mil server for question development, and other information that does not deal with Military Value Scoring Plans, data call responses, scenarios, possible alternatives, or Candidate Recommendations.

9. SOP Review

This SOP should be reviewed quarterly to ensure individuals are following the guidelines and that necessary updates are made.


George Mayer
RADM USN

Draft Deliberative Documents – For Discussion purposes only
Do not release under FOIA

Addendum 2 to E&T JCSG-PDE SOP dated 27 October 2004

Scenario Tracking

Scenario data requests will be submitted to the appropriate service PDE representative for processing. Each service will formalize their own methodology for data requests however, this will not preclude submission and retrieval of data via courier and electronic disks (see Addendum 1). Email is not authorized for any scenario data. The following sections apply to specific scenario data call ICP issues

1. OSD Portal

- a. The PDE subgroup will designate one Point of Contact and one alternate to be given access to the Air Force Scenario Data Portal. These individuals will be able to deliver electronically (through secure FTP technology) scenario data worksheets and any other applicable information for the services to conduct its data calls. In addition these designated individuals will be able to retrieve from the portal site all completed scenario information. The designated POC and alternate will be given separate user names and passwords to be managed by the Air Force BRAC office.

2. Secure Facsimile (FAX) Instructions

- a. Scenario data may be sent via fax machine only when positive voice confirmation is achieved prior to transmittal. The sender will ensure the receiver is present at the receiving fax machine with a phone conversation. Upon completion of data transmittal, the receiver will contact the sender to confirm receipt and number and quality of pages sent. All data sent will be logged in accordance with the procedures in Section 4 of the Internal Control Plan.

3. Scenario Tracking Spreadsheet

- a. The development of scenarios occurs in three stages: ideas, proposals and scenarios. Ideas are formulated at the PDE subgroup level and as the subgroup is a nondeliberative body, ideas are not subject to BRAC tracking procedures other than entry into the JCSG Scenario Tracking Tool. Proposals are submitted to the JCSG deliberative body for approval or disapproval with the appropriate date and accompanying commentary. Scenarios are approved proposals and receive an official E&T scenario tracking number as generated by the OSD Scenario Tracking Tool.

- b. The tracking spreadsheet will be updated once a week, typically after the E&T Principles meeting. The update will be made at one location (BRAC office, Rosslyn, VA) by a subgroup member and given to the E&T scenario representative.
- c. Electronic copies of each week's spreadsheet are kept on the PDE shared folder in Rosslyn, VA.

4. Scenario ISG Tracking Tool

- a. The ISG Scenario Tracking Tool is a Microsoft Access data base tool that allows for convenient deconfliction of all approved scenarios. When a proposal is approved by the E&T principles, the new scenario must be entered into the ISG tracking tool in order to receive its official number.
- b. The entry must include a detailed description of the scenario as well all gaining and losing installations and activities affected.
- c. All updates to the Tracking Tool will be complete by noon of the day following the JCSG Principles meeting.

5. Criteria 6,7,8 Points of Contact

- a. For Criteria 6 (Economic Impact of the Losing Installation) the Point of Contact is LtCol. Greg Moore.
- b. For Criteria 7 (Community Impact of the Scenario) the Point of Contact is Mr. Frank Petho.
- c. For Criteria 8 (Environmental Impact of the Scenario) the Point of Contact is COL. Robert Grubbs.

6. Weekly Disc Back-Ups

- a. All work conducted for a given week is stored in a unique floppy disc or CD-Rom. The work consists of but is not limited to, Military Value updates, Capacity updates, weekly slide briefings and Requests for Clarifications.
- b. The updates are placed in an electronic folder every Friday. One copy is saved in the PDE shared drive, the other is saved in the discreet floppy disc or CD-Rom.



Thomas C. Matney
BG, USA
Chair, E&T JCSG-PDE

Addendum 1 to E&T JCSG-PDE SOP dated 2 August 2004

RECEIPT OF DATA CALL INFORMATION FROM E&T JCSG CHIEFS

- a. E&T JCSG Chiefs will provide the E&T JCSG PDE subgroup with the BRAC data call information via CD. The PDE POC is designated the individual authorized to transport the BRAC information. While transporting BRAC information, media should be appropriately covered with close hold cover sheet and protected from possible disclosure.
- b. Upon arrival back at the PDE work site, Room 1B474A, Pentagon, the CD will be logged according to the PDE SOP. The POC will copy the CD onto the PDE Stand Alone computer hard drive. The PDE POC will verify everything was copied from the CD to the hard drive. The CD will then be secured in accordance with PDE SOP. This CD will not be used again unless the file on the Hard Drive should become corrupt. Paper copies of the working data from the hard drive will be logged and distributed to PDE members according to PDE SOP. Only the Chair, POC, and members designated in writing by the Chair are authorized to make copies of the BRAC information. PDE members are required to secure any paper copies of BRAC data according to PDE SOP.

TRANSFER OF INFORMATION INTO THE SUBGROUP ANALYSIS TOOL

- a. The PDE POC designates the PDE data manager/administrator and primary Service PDE members authority to take the information off the hard drive and input it directly into the PDE analysis tool. Each member is responsible for verifying the accuracy of the BRAC information entered into the tool. PDE members who enter BRAC information into the tool must have another PDE member verify information accuracy. The DODIG is responsible for performing spot checks on the accuracy of the BRAC data transfer. If data entry errors are discovered, the member committing the error or POC will make immediate corrections and the change revalidated for accuracy.

RECEIPT OF SUPPLEMENTAL DATA CALL INFORMATION FROM E&T JCSG CHIEFS

- a. E&T JCSG Chiefs will provide the E&T JCSG SST subgroup with the BRAC supplemental data call information via CD. The PDE POC is designated the individual authorized to transport the BRAC information. While transporting BRAC supplemental information, media should be appropriately covered with close hold cover sheet and protected from possible disclosure.

- b. Upon arrival back at the PDE work site, 1B474A, Pentagon, the CD will be logged according to the PDE SOP. The POC will copy the CD onto the PDE stand alone computer using the hard drive. The supplemental information will be stored in folders on the hard drive, BRAC file as follows:
 - Data Call Number
 - (a) Army
 - i. Question 103 (Example)
 - ii. Question 108 (Example)
 - (b) Navy/Marine Corps
 - (c) Air Force
 - (d) Defense Agencies

The PDE POC will verify everything was copied from the CD to the hard drive. The CD will then be secured in accordance with PDE SOP. This CD will not be used again unless the file on the hard drive should become corrupt. Paper copies of the hard drive BRAC Supplemental information will be logged and distributed to PDE members according to PDE SOP. Only the Chair, POC, and members designated in writing, are authorized to make copies of the BRAC Supplemental information. PDE members are required to secure the paper copies of BRAC supplemental data according to PDE SOP.

- c. The PDE POC is responsible for incorporating supplemental data into the hard drive BRAC files. The PDE POC will identify the specific question, data element, and response to be changed. In the electronic files (access and MS Word), the PDE POC will key enter updated response in the appropriate location(s) and in the MS Word add a footnote that includes the date, log number and change. For PDF files, the PDE POC will attach a comment (date, log number and change) to the specific PDF file that is being updated. A primary Service PDE member will verify the supplemental data was updated correctly into the hard drive BRAC files. The DODIG is responsible for performing spot checks on the accuracy of the BRAC supplemental data transfer. If data entry errors are discovered, the POC will make immediate corrections and the change revalidated for accuracy. The POC will identify to the primary Service PDE members that supplemental data has been received and changes are required in the data tool.

- d. The PDE POC designates the PDE data analyst and primary Service PDE members authority to take the information off the hard drive BRAC supplemental file and input it directly into the PDE analysis tool. Each member is responsible for verifying the accuracy of the BRAC supplemental information entered into the tool. PDE members who enter BRAC supplemental information into the tool must have another PDE member verify information accuracy. The DODIG is responsible for performing spot checks on the accuracy of the BRAC data transfer. If data entry errors are discovered, the member committing the error or POC will make immediate corrections and the change revalidated for accuracy. The PDE data analyst and primary Service PDE members must review all analysis tools to determine all areas impacted by the supplemental information.
- e. The PDE POC will designate the personnel authorized to respond to RFQs (Request for Clarification) from the Military Service Departments and various DoD agencies. OSD BRAC has created a query tool to assist in collecting RFQs and disseminating to the correct subgroups. The query entries are made by designated personnel within the MilDep and forwarded to the E&T JCSG via email. The JCSG representative will then forward to the appropriate subgroup representative for response (see E&T ICP for more details). The Subgroup representative will have two business days to provide a response via email.
- f. All supplemental data and data base “refreshes” will be delivered to the subgroup by means of a CD-ROM. The disk will be provided to the E&T JCSG representative, who will make one (1) copy for every subgroup. The PDE designee will receive the subgroup copy, log it and copy a working version to all PDE PCs at 1401 Wilson Blvd. For details on network security within the BRAC office at 1401 Wilson BLVD see ref. 6 (SOP for BRAC Office). Once a week the designated member of the PDE subgroup will bring the archival CD-ROM disk over to 1B474A, in the Pentagon, to update the working copy at that location.



Thomas C. Maffey
BG, USA
Chair, E&T JCSG-PDE

**Standard Operating Procedures
for the
Education and Training Cross-Service Group
(E&T JCSG)
Base Realignment and Closure (BRAC) 2005**

**Standard Operating Procedures for the
Education and Training Joint Cross-Service Group (E&T JCSG)
Base Realignment and Closure (BRAC) 2005**

1. PURPOSE

This document contains important information on the Standing Operating Procedures (SOP) related to controls necessary to safeguard the BRAC 2005 deliberative data, documents, decisions, and recommendations for the E&T JCSG.

2. REFERENCES

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.*

Defense Base Closure and Realignment Act of 1990 (Public Law 101-510, as amended).

Memorandum, Secretary of Defense, 15 November 2002, Subject: Transformation Through Base Realignment and Closure.

Message, Secretary of Defense, 13 February 2003, Subject: Public Affairs Guidance (PAG) – Transformation Through Base Realignment and Closure (BRAC 2005).

Message, Secretary of Defense, 20 November 2003, Subject: Public Affairs Guidance (PAG) – Transformation Through Base Realignment and Closure (BRAC 2005).

3. KEY POINTS OF CONTACT

The E&T JCSG shares office suite space with several JCSGs and sub-groups. Each JCSG is responsible for their own security. Each sub-group is responsible for providing adequate controls and management oversight to protect against the release of their sub-group's information to unauthorized personnel. The E&T JCSG key points of contacts include:

- a. E&T JCSG Chiefs and primary points of contact (POC): Ms. Nancy Weaver, (703) 696-6435 Ext 206 and Mr. Robert Howlett, OSD P&R, Ext 319.
- b. E&T JCSG Senior Analyst: Mr. Mark Horn, (703) 696-6435 Ext 209.
- c. Office Manager for Suite 501: Mr. Jack Hoggard, (703) 696-6435 Ext 201.
- d. Building Security Manager: Mr. Tom Prudhomme, (703) 601-2554 Ext 103.
- e. Computer Support Staff: Ms. Janet LaFave or Ms. Wanda Brisco, (703) 696-9432.
- f. Data/Document Control Manager/Analyst: Ms. Marsha Warren, (703) 696-6435 Ext 290.
- g. E&T JCSG Security Manager: YNC Tom Seaker, (703) 696-6435 Ext 209.
- h. E&T JCSG Executive Administrative Assistant: YNC Tom Seaker, (703) 696-6435 x209.

4. STORAGE / ACCESS REQUIREMENTS

- a. Physical location used to store data. All BRAC 2005 data will be securely stored at the E&T JCSG Federal Government office space at 1401 Wilson Boulevard, Suite 502, Rosslyn, Virginia 22209.
- b. Physical security for the location. The entrance to the office space is secured by locks on all access doors and the main door is controlled by an electronic badge access reader. Individuals without DoD swipe access badges are escorted and are required to utilize the Visitor Register log (located at the doorway for Room 550). Access is controlled by the Office Manager or the E&T JCSG Security Manager to the E&T JCSG staff. An Access Log is maintained by the E&T JCSG Security Manager identifying who has access to Suite 502.
- c. All Swipe Card requests shall be approved by the E&T JCSG Chief prior to its submission to the Security Manager. The paperwork required to obtain the Swipe Access Card is maintained on file with the Office Manager. The following are the requirements to hold a Swipe Access Card (exceptions limited to those approved by an E&T JCSG Chief).
 - (1) Swipe Card Access. Requirements for eligibility for swipe access to suite 502:
 - i. Maintain a permanent seat and/or an email account access in this facility.
 - ii. POCs must provide the E&T JCSG Security Manager a written request 48 hours prior required access.
 - iii. Provide the Security Manager with the following information:
 1. Full name
 2. Social Security Number
 3. Copy of signed Non-disclosure Agreement
 - iv. Permission granted by one of the E&T JCSG Chiefs.
 - v. E&T JCSG Security Manager submits the required Excel spreadsheet to the Office Manager (zone 615 access request form is located on the E&T JCSG Shared drive (S:\Electronic Filing System\Administrative\Zone Access)). (All routing information is located at the bottom of the form).
 - (2) Physical Access. Individuals receiving access to Suite 502 must be part of BRAC 05 and have a need to know E&T JCSG BRAC information. First time individuals must be escorted by subgroup POCs and are required to provide a signed Non-disclosure Agreement to the E&T JCSG Security Manager for E&T JCSG files. Any individuals present that are not on E&T JCSG Subgroup Membership phone roster will not be granted access.
- d. Hard copy storage. Special containers to store hard copy files are not required within the E&T suite since the suite is secured behind locked doors, which limits access to authorized personnel. However, E&T staff members will ensure their documents are properly protected, safeguarded, and stored in locked file cabinets and/or safes when not in use.

- e. **Soft copy storage.** Softcopy files are maintained on a WHS secured server. This dot Mil server is password protected and only the necessary system administrators and E&T JCSG members have access to the files. WHS staff performs intrusion detection monitoring of the network backbone and the System Administrators conduct periodic reviews of the systems log files to detect and prevent unauthorized access to the network. The E&T JCSG Security Manager requires all WHS administrators to sign Non-disclosure Agreements.

Note: WHS support team will be responsible for performing backups of the server and E&T JCSG files. Once a week a system backup is created, archived, and maintained at an off-site location (52 weekly tapes are maintained on file). Additionally, daily partial backups are conducted to protect work production.

5. DOCUMENT CONTROL

- a. **Transportation of Information.** E&T JCSG Chiefs, Security Managers, Data Managers, and Executive Administrative Assistants are the only individuals authorized to transport original documents, computer disks, etc. Documents must be concealed and have "CLOSE HOLD" denoted on the outer covering.
- b. **Preserving documents.** All master files and documents shall be maintained in an electronic (normally .PDF) or paper format. When required for reference material, for the E&T JCSG office, paper copies may be maintained at the discretion of the staff member.
- c. **Tracking documents.** All deliberative documents/information produced by or submitted to the E&T JCSG (e.g., Official Correspondence, Data Call databases, change records, scenarios, possible alternatives scenarios, or recommendation candidates) will be assigned sequential control numbers by the E&T JCSG Executive Administrative Assistant and entered in to the electronic documents log (control number, copy number (copy 1 of N copies if applicable), title, subject, date, who accessed the data, and date issued. Prior to any documents being copied, coordination must be made with the E&T JCSG Executive Administrative Assistant to determine if the document needs to be logged. The E&T JCSG Executive Administrative Assistant will document copied information into the Control Document Log as required.
- d. **Access to BRAC original information.** E&T JCSG members will work only with a copy of the original BRAC information. Only the E&T JCSG Chair, the E&T JCSG Chiefs, Security Manager, Senior Analyst, Data Manager/Analyst, and Executive Administrative Assistant have access to the original information provided by OSD BRAC. Upon receipt of the original data, copy(s) will be made by the E&T JCSG Executive Administrative Assistant. The original will be locked up in a file cabinet while the copy(s) will be used by the subgroups for analysis. Copies will be assigned control numbers as stated above.

Note: JCSG Meeting Minutes shall be filed, in binders and electronic format, by date vice the sequential control number system described above.

- e. Copies of Information. All copies made for in-house (e.g. meetings, briefings) purposes will be collected the same day by the E&T JCSG Chiefs, Security Manager, or Executive Administrative Assistant and destroyed weekly through the local burn center. At the discretion of the E&T JCSG Chiefs, signatures may be required for specific copies that are transferred to other group, subgroups or originations.
- f. Information Access. Access to copies of deliberative and/or draft deliberative documents will be restricted to those individuals who have signed Non-disclosure Agreements that are on file in Suite 502 and on a need to know basis. All deliberative documents are “CLOSE HOLD” information and shall be maintained in the E&T JCSG secure office space. Authorized individuals who remove copies of deliberative and/or draft deliberative documents (electronic or paper) from E&T JCSG secure office space must first obtain permission from the E&T JCSG Chiefs or Security Manager and sign for the material in a sign-out log maintained by the E&T JCSG Executive Administrative Assistant. 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 Defense Base Closure and Realignment Commission shall be forwarded to Military Department BRAC Authority concerned, or the DUSD(I&E).”

- g. Information Disclosure. 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.
- h. Computers are provided in the E&T JCSG offices by WHS. These computers are password protected and users must change their password every 90 days. Passwords must contain at least 8 characters, one special character, one number and one capital letter. Users may not use a previous password for at least 10 password changes. Passwords should not be written down or shared with anyone.
- i. All employees must lock the computer whenever the individual leaves their work area. The individual will log-off the computer at the end of each duty day. Computers must be shut down on Friday evenings.
 - (1) 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.
 - (2) 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.

- j. Document Destruction. As required, BRAC documents will be returned to the E&T JCSG Executive Administrative Assistant for disposition. It is each person's responsibility to ensure all other BRAC related documents not under document control are placed into the burn bags. The DoD Incinerator organization is responsible for destroying classified and unclassified documents, IAW Administrative Instruction 26, Chapter 9.
- k. Information Security Breach. All precautions must be taken to avoid loss/unauthorized release of "CLOSE HOLD" information that is considered or produced by the E&T JCSG and its subgroups. Attention to detail and training are the best preventative measures to avoid a security breach. However, if and when a security breach incident occurs, the following checklist shall be used:

The individual identifying the breach shall:

1. Conduct an immediate search of the local area and question personnel in the vicinity.
2. Notify the E&T JCSG Chairs Persons and the Security Manager.

The E&T Security Manager shall:

1. Conduct an exhaustive search in the vicinity of the document's/CD's last known location.
2. Assess the nature/impact of the loss/unauthorized release of the "CLOSE HOLD" information.
3. Report incident status to the E&T JCSG Chairs Persons.

The E&T JCSG Chair Persons shall:

1. Review the incident.
2. Expand the search/open an investigation concerning the incident, as seen fit.
3. Assess potential damage/publicity that could be associated with the incident.
4. At their discretion, inform all appropriate authorities of the nature, extent, and resolution of the security breach.

6. FACSIMILE

The use of facsimile machines to transmit information such as Military Value Scoring Plans, data call questions and responses, scenarios, possible alternatives, or recommendation candidates is not permitted. Information not dealing with Military Value Scoring Plans, data call questions and responses, scenarios, possible alternatives, or recommendations may be faxed to authorized recipients. Individuals are responsible for logging in the appropriate information into the "Document Fax Log". Care will be taken to ensure that the facsimile machine is monitored during transmission and receipt to preclude any compromise of sensitive information. The procedure is that contact between the individuals sending/receiving the fax must be made and that each individual must be present at the FAX to control transferred documents and confirm receipt. A sign will be posted on the facsimile machine stating the requirement for monitoring transmissions. This is not the normal means of communication.

7. MINUTES

The E&T JCSG members will make all deliberative decisions at the E&T JCSG deliberative meetings, not at the subgroup level. Minutes for all JCSG deliberative sessions will be signed by the Chairman of the E&T JCSG and maintained in a secure office space. Minutes of subgroup or team meetings are not required unless they are deliberative. If minutes are taken for subgroup or team meetings, the original will be maintained in the secure office space. E&T 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 review of the Minutes is accomplished by the E&T JCSG Chiefs, DoDIG, Subgroup POCs, BRAC and E&T JCSG Chair. A literal transcript of the meeting is not required. The OSD BRAC and DoD IG offices will also maintain a copy of these minutes.

8. RECORD KEEPING

The E&T JCSG Executive Administrative Assistant will develop and maintain records in a timely manner of all of the following types of information:

- a. Signed Nondisclosure Agreement.
- b. Descriptions of how E&T JCSG BRAC 2005 policies, analyses, and recommendations were developed. To include, but not limited to: directives from higher authority in the form of memorandums, policy statements and such that directly affect the E&T JCSG policies/business practice.
- c. Minutes of all deliberative meetings of the E&T JCSG.
- d. All data, information, and analyses considered in making E&T JCSG BRAC 2005 recommendations.
- e. List of individuals and titles, which will be kept updated, associated with the E&T JCSG is attached at Appendix A.

9. 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 data used during the BRAC process needs to be marked with appropriate headers and footers as seen under "Office Procedures For Correspondence" below.

10. 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 E&T JCSG subgroups will take all press, public, or Congressional inquiries without comment and forward with proposed answers to the

E&T JCSG Coordination Team. Forwarded inquiries should include the publication name, reporter's name, and deadline.

- b. If the inquiry is from the public, 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 E&T JCSG Coordination Team will forward Congressional inquiries to OSD Legislative Affairs for response.

11. 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 Military Value Scoring Plans, data call responses, scenarios, possible alternatives, or Candidate Recommendations. However, use of e-mail to transmit information that does deal with Military Value Scoring Plans, data call responses, scenarios, possible alternatives, or Candidate Recommendations is prohibited.

12. PERFORMING ANALYSIS

- a. Analysis of certified data, scenarios, etc. must be conducted at the E&T JCSG secure office space or the appropriate subgroups' secure facilities.
- b. Specified E&T JCSG staff will perform the analysis.

13. OFFICE SECURITY

- a. The E&T JCSG office space is secure and the doors must remain closed and locked at all times. The last person to leave the office will do a security check and fill out the security checklist before departing. It is each individual's responsibility to ensure that in the evening before leaving: desks are cleared of deliberative papers, trash receptacles contain no BRAC papers, office windows are closed and locked, and that they are logged off of their PCs.
- b. Visitors (all non full-time employees) must sign into the "Visitor Register", 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 2005 information. Office personnel are required to stop and question strangers and report suspicious activity immediately to the E&T JCSG Coordinators and/or Security Manager.

14. OFFICE PROCEDURES FOR CORRESPONDENCE

- 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 Executive Assistant.
- 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 it is updated.

15. RECEIPT OF DATA CALL INFORMATION FROM OSD BRAC

- a. OSD BRAC will provide E&T JCSG Chiefs, Senior Analyst, Data Manager/Analyst or Executive Administrative Assistant data call questions and responses via disk/CD in Access, MS Word, and PDF format. Upon receipt, the Senior Analyst, Data Manager/Analyst, or Executive Administrative Assistant will copy original data call information to the E&T JCSG shared drive that is only accessible by the E&T JCSG Chiefs, Security Manager, Executive Administrative Assistant, and Data Manager. The file on the shared drive will only be used to make copies. The master disk/CD is being copied in case the disk/CD gets damaged. The disk/CD will only be used again if a problem occurs with the information on the shared drive. The E&T JCSG Executive Administrative Assistant will verify that everything was copied from the master disk/CD to the shared drive.
- b. The E&T JCSG Senior Analyst, Data Manager/Analyst or Executive Administrative Assistant will make copies from the shared drive to a CD that will be distributed to each of the subgroups. The E&T JCSG Executive Administrative Assistant will verify all information was copied before distributing out CDs. Authorized individuals identified by the subgroup POC responsible for carrying information must follow procedures described above in section 5.d.
- c. Each E&T JCSG subgroup will be responsible for establishing procedures on how they will control all information removed from Suite 502.

16. TRANSFER OF INFORMATION INTO THE SUBGROUPS' ANALYSIS TOOL

Each E&T JCSG subgroup will take the information received on the disk/CD and input it directly into their analysis tool. Each E&T JCSG subgroup is responsible for establishing procedures that verify data was accurately copied from CD into their analysis tool.

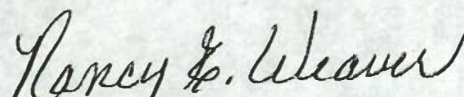
17. RECEIPT OF SUPPLEMENTAL DATA CALL INFORMATION FROM OSD BRAC

- a. Supplemental data call information will come in from OSD BRAC as required. OSD BRAC will provide E&T JCSG Chiefs or Executive Administrative Assistant supplemental information via soft or hard copy. Upon receipt of hard copy information, the E&T JCSG Executive Administrative Assistant will scan original supplemental information to the E&T JCSG shared drive that is only accessible by the E&T JCSG Chiefs, Security Manager, Executive Administrative Assistant, and Data Manager. The files on the shared drive will only be used to make copies. The original supplemental hard copy is being scanned in case the hard copy gets damaged. The E&T JCSG Executive Administrative Assistant will verify that scanned file is readable on the shared drive.
- b. If a Subgroup receives certified data directly from a Service, the Subgroup shall turn over the data to the E&T JCSG CT. In turn the E&T JCSG CT shall turn that same data over to OSD BRAC Data Manager.
- c. The original supplemental hard copy information will be maintained in accordance with paragraph 5 (Document Control). Binders will be set up as follow:
 - Data Call Number
 - (a) Army
 - i. Question 103 (Example)
 - ii. Question 108 (Example)
 - (b) Navy / Marine Corps
 - (c) Air Force
 - (d) Defense Agencies
- d. The scanned supplemental information will be stored in folders on the shared drive broken down as follow:
 - Data Call Number
 - (a) Army
 - i. Question 103 (Example)
 - ii. Question 108 (Example)
 - (b) Navy / Marine Corps
 - (c) Air Force
 - (d) Defense Agencies
- e. The E&T JCSG Executive Administrative Assistant will make copies of supplemental data from the shared drive to a CD that will be distributed to each of the subgroups as appropriate. The E&T JCSG Executive Administrative Assistant will verify all supplemental data was copied before distributing out CDs. Authorized individuals identified by the subgroup POC responsible for carrying information must follow procedures described above in section 5.d.
- f. The E&T JCSG will not update the copied original data call information on the shared drive with the supplemental data. The E&T JCSG subgroups will be responsible for updating their copy of the original data call information with all supplemental data

received. Each E&T JCSG subgroup will be responsible for establishing procedures on how they will incorporate supplemental data received into their copy of the original data call information and analysis tool.

18. Fire Bill. In the event of a fire, all personnel shall vacate the building immediately. The E&T Rally Point location is located on the corner of Oak and 18th Street (across the road from the main entrance).

19. SOP Review. This Standard Operating Procedure should be reviewed quarterly to ensure individuals are following the guidelines and that changes are made appropriately.



Nancy E. Weaver

Nancy E. Weaver
Education and Training, Joint Cross
Service Group Chief and Primary
Point of Contact

the PDE subgroup who have signed the nondisclosure agreement will be given the lock combination. The E&T JCSG BRAC office at Rosslyn will confirm to the security SOP for that area (See Ref. 6), in addition the following courier requirements will be in place for movement of data between the two locations:

(i) To the greatest extent possible, only electronic disks will carry information between the two locations. If paper copies must be carried, it shall be in strict accordance with section 4.b below, and only with the approval of the Subgroup chair or the designated POC.

(ii) Only predestinated courier disks (Zip, floppy or CD-ROM) will be utilized for transportation of data between the locations. (Draft Deliberative Document – For Discussion Purposes Only Do Not Release Under FOIA).”

b. Additional security requirements for storage:

(i) Room 1B474A and the E&T JCSG workspace located at 1401 Wilson Boulevard, Rosslyn, VA will be the only designated PDE BRAC data storage, and analysis work area. 1B474A is a secure conference room within the J-7 Joint Education and Training Division work area.

(ii) All BRAC working papers will be stored in 1B474A and Rosslyn location a daily basis. No data/data analysis (to include notes/note pages) will leave the 1B474A or Rosslyn location without logging out with stated purpose.

(iii) Standard Form 702 will be used to document access to security containers.

(iv) Data may be stored on individual computers only on disk or hard drive not connected to the network or with a laptop or removable hard drive that can be removed and secured. Computers will be password protected and have password protected screen savers.

(v) Data will not be transmitted over the internet/network. When data analysis is conducted via automation; the computer will have a removable hard drive, or utilize a laptop that can be disconnected from the network. All PC workstations will not have external connectivity through either physical or logical connections.

(vi) Computers will comply with standard Department of Defense computer security requirements.

- o Data will be secured and requests for data will be controlled to assure that only individuals with a bona fide need to know are granted access.
- o Intranet Security and Access Controls: All PDE data and products shall be kept and worked on in the designated PDE controlled access workspace in room 1B474A and 1401 Wilson Blvd. Computers used by the subgroup at 1B474A will remain stand-alone and will not be connected to any networks. No work will be done on computers connected to Intranet or Extranet services except if conducted at designated work stations at Rosslyn location.

4. Control Requirements:

a. Data input will be inventoried, dated, logged assigned a control number and designated “Original Copy”. The PDE Subgroup Chair and his designated Point of Contact (POC) are the only ones with access to the “Original Copy”. A “Master Copy” of the Original will be re-produced and is the main source of data for conducting analysis. Additional copies will be made on a limited basis to support questions, notes, and analysis with prior approval of the PDE Subgroup Chair. The same control number will be used for each copy, annotated with copy number and total number of copies re-produced (e.g. Control # 101A –1 Of 10/2 Of 10).

b. Additional Control Requirements:

(i) Log and/or sign-in sheets are maintained by the PDE Subgroup designated POC to control all data and personnel.

(ii) Logging procedures: Two separate logs are utilized

- Log #1: Information review and analysis only in the data storage area location where the “Master Copy” is stored. Copies should be limited but, can be re-produced and must be returned to POC prior to departing data storage area.
 - Name (Last, First, MI)
 - Non-disclosure on file (yes/no), if no access is denied
 - Date (dd/mmm/yy) signed out (to work in the designated data analysis work area).
 - Time (24 hour clock)
 - Date (dd/mmm/yy) returned
 - Time (24 hour clock)
 - Rank, Civilian (Title, grade)
 - Organization
 - Description of information
 - Purpose (why access is requested)
- Log #2: Information copied for removal
 - Name (Last, First, MI)
 - Non-disclosure on file (yes/no) If no access is denied
 - Date (dd/mmm/yy) copied
 - Time (24 hour clock)
 - Rank, Civilian (Title, grade)
 - Organization
 - Number of Pages copied
 - Description of information
 - Reason for copy
- Log #3: Access checks log; Recap of Log 1 and 2 on monthly basis. Purpose is for POC to run periodic checks ensuring only authorized BRAC personnel gain access to facility and data.

Recap of information copied, information leaving facility, and control measures.

- Date (by month)
- Data requests for analysis in designated storage area
- Data requests to be copied/removed
- Rank, Civilian (Title, grade)

(iii) Original data, copies, notes, or computations will not be removed from the secure area without prior approval of the PDE Subgroup Chair.

- If information is to be removed, the PDE Subgroup chair or his designee will assure all documents are properly marked with BRAC header/footer information (Draft Deliberative Document – For Discussion Purposes Only Do Not Release Under FOIA).
- If personnel are authorized to leave the BRAC Controlled Data Secure Area(s) with BRAC data, the data and cover sheet will be in manila envelope and/or sufficient containers to secure information. Personnel transporting such material must have the ability to restrict access to the data at interim and final destinations. Taking data out of the secure area is the exception not the norm.
- The use of e-mail for discussion, notes, and computations is prohibited. This includes in addition to notes, data regarding scenarios, alternatives, recommendations, military value scoring plans and capacity analysis.

5. Access Requirements:

a. Data access is limited to members of the JCSG- E&T PDE Subgroup and to those the Chair designates in accordance with sign-in procedures listed above. The Chair will maintain a list of individuals granted access to the information within facility/secure area. The subgroup POC is responsible for opening and securing the data/facility. The list is modified only with the approval of the Subgroup Chair. The subgroup POC will maintain a list of individuals who have signed a Non-Disclosure Agreement. The Subgroup POC will serve as the point of contact for access and availability of data. Each primary Subgroup member (service designees) will have equal access to the data. However, the Subgroup POC will make the determination whether varying levels of access are authorized for support members based upon the situation.

b. Additional Access Requirements:

- (i) An access authorization list of personnel with authorized access to facility/secure area is maintained by PDE subgroup POC and checked when access is requested.
- (ii) No access is granted if the individual is not on the approved list.
- (iii) Non-disclosure agreements are maintained as backup documentation to the approved access list.

(iv) One time access to data/secure area for Subject Matter Experts (SME) is granted by the Chair. SME are not authorized to remove, take any of data in any form, (hard copy, notes, electronic) from the data storage area. Subgroup POC will assure all SMEs have signed non-disclosure statements.

6. Other Requirements:

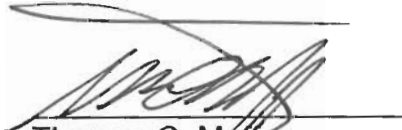
a. All data, including copies/version in any form are centrally stored. To prevent unauthorized access to data submissions, the suite is locked when not in use.

b. Other Requirements:

(i) SOP's will be reviewed and updated as required.

(ii) If additional information is collected (i.e from subsequent data calls) the information will be handled in the same manner as described above.

(iii) Corrected or replaced information will be annotated in the appropriate logs, with positive control kept of all versions. Old versions will be destroyed only upon approval of subgroup POC and then in accordance with section 4.a.



Thomas C. Mahey
BG, USA
Chair, E&T JCSG-PDE


FOR
EDUCATION AND TRAINING JCSG
RANGE SUBGROUP FOR
SAFEGARDING BRAC 2005 DATA

ADDENDUM 5

29 Apr 2005

Subject: Addendum 5 to ICP SOP

1. Addendum 5 to the Internal Control Plan (ICP) to the Range Subgroup SOP for the safeguarding of BRAC data is: The addition of transportation requirements between the JCSG in Rosslyn and the Range Subgroup in the Pentagon (1E121).
2. I approve addendum 5 to the ICP SOP.
3. Alternate E&T JCSG Range Subgroup working POC is Mr. Robert Lepianka, 703-692-6427, DAMO-TRS.


for James. B Gunlicks
Deputy Director of Training

**STANDARD OPERATING PROCEDURES (SOP)
FOR
EDUCATION & TRAINING JCSG
RANGES SUBGROUP
FOR SAFEGARDING BASE REALIGNMENT AND CLOSURE (BRAC 2005) DATA**

30 Jan 2002

1. Purpose: The Office of the Secretary of Defense Internal Control Plan (ICP) establishes the policies and responsibilities for the protection of **DATA TO PREVENT PREMATURE DISSEMINATION**. It is the responsibility of each Joint Cross Service Group and its respective subgroups to ensure internal controls and a Standard Operating Procedure (SOP) is in place for handling information received in data calls. The subgroup chair of each designated BRAC group will ensure all assigned members of the group have signed non-disclosure statements and are informed that no internal deliberation or data will be discussed or shared with anyone outside their group. The goal is to ensure accuracy, completeness, and integration of all information and analytical processes upon which BRAC 2005 recommendations are based and to limit the possibility of premature or improper disclosure. This includes inadvertent dissemination of BRAC information through any means.

References:

- Memorandum, Secretary of Defense, 15 November 2002, Subject: Transformation through Base Realignment and Closure.
- Memorandum, Secretary of Defense, 13 February 2003, Subject: Public Affairs Guidance (PAG) - Transformation through Base Realignment and Closure.
- 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.

2. Administrative Responsibilities:

a. Storage Requirements: Store data in DAMO-TRS Rm 1E121, Pentagon, Arlington Virginia for use by the Training sub-working groups, and in Chief of Naval Operations (OPNAV), Director, Test and Evaluation and Technology Requirements (N091), Rm 3400, Presidential Tower, Crystal City, Virginia, for use by the Test and Evaluation sub-working group (T&ESWG). These will be the only authorized storage and data analysis work locations. Both buildings are badged with both Military and uniformed guards controlling access to the buildings. Both offices are protected by either card lock or tumbler lock and a cipher keypad. Army G-3 DAMO Admin is responsible to ensure that the codes and combinations to Rm 1E121 are changed every 90 days for Rm 1E121, and N091 is responsible for codes and combinations changes for Rm 3400. It is the responsibility of the E&T JCSG Ranges Subgroup working lead POC, Mr. Thomas Macia 703-692-6410, to ensure that DAMO administration is alerted to the departure or addition of any permanent Ranges Subgroup team members. Designated alternate E&T JCSG Ranges Subgroup working POC is Mr. Robert Lepianka, 703-692-6427. It is the responsibility of Mr. John Foulkes, 703-695-8996, to inform N091 administration of the departure or addition of any permanent T&ESWG member.

b. Additional security requirements for storage:

- ❖ Room 1E121, DAMO-TRS and Rm 3400, N091, will be the only designated BRAC data storage areas, analysis work areas, and the only locations to work with the BRAC data. Rm 1E121 and Rm 3400 are secure areas that have secure conference rooms for data analysis discussions.

Draft Deliberative Document – For Discussion Purposes Only
Do Not Release Under FOIA

- ❖ BRAC 2005 questions will be stored in lockable, key controlled, steel, standard issue 2-4 drawer file cabinets at each location (1E121 and 3400) on a daily basis. NO data/data analysis (to include notes/note pages) will be done anywhere other than these Ranges Subgroup designated BRAC facilities (1E121/3400).
- ❖ Standard Form 702 will be used to document access to security containers.
- ❖ BRAC Data (i.e. Mil Val) may be stored on individual computers only on disk or hard drive which is not connected to the network or with a removable hard drive that can be removed and stored in the Ranges Subgroup designated storage facilities (1E121/3400).
- ❖ Computers will be password protected and have password protected screen savers.
- ❖ Data **Will Not** be transmitted over the internet/network. If/when data analysis is conducted via automation; the computer will have a removable hard drive, or be a laptop that can be secured/disconnected from the network.
- ❖ Computers will follow standard DoD computer security requirements.
 - Data will be secured and requests controlled to ensure that only individuals with a bonified need to know are granted access.
 - Intranet Security and Access Controls (1E121): The OPSLAN Intranet sites are protected from external access by a firewall and proxy server. These sites are accessible only by users of OPSLAN and trusted Pentagon HQDA networks.
 - Extranet Services (1E121): The DCS G3 CIO office maintains servers and provides support for publishing external (NIRPNET/Internet accessible) sites. Typically DCS G3 sites are provided security and access controls IAW Army and DoD guidance.
 - Extranet Security and Access Controls (1E121): The OPSLAN Extranet servers are designed as non-public servers. Sites on the server are protected by authentication, (Public Key Infrastructure) encryption or by domain (.mil) restrictions.
 - Rm 3400 will use only standalone computers and all data will be transferred via CD-ROM or discs which will remain in the space and be stored in lockable file cabinets when not in use.

3. Control Requirements:

a. Data Call replies will be inventoried, dated, logged assigned a control number and designated "Original Copy." E&T JCSG Ranges Subgroup working lead POC Mr. Thomas Macia 703-692-6410 and/or E&T JCSG Ranges Subgroup working alternate POC (Mr. Robert Lepianka) are the only ones with access to the "Original Copy". Two "Master Copies" of the Original will be re-produced and will be the main source of data for conducting analysis in Rm 1E121 and Rm 3400. Additional copies will be made on a limited basis to support questions, notes, and analysis with prior approval of the E&T JCSG Ranges Subgroup working lead POC. The same control number will be used for each copy, annotated with copy number and total number of copies re-produced (e.g. Control # 101A -1 Of 10/2 Of 10).

b. Additional Control Requirements:

- ❖ Log/sign-in sheet will be maintained by E&T JCSG Ranges Subgroup working alternate POC (Mr. Bob Lepianka) to control all data and personnel for Rm 1E121 and by T&ESWG alternate POC (Mr. C. Buchanan) for Rm 3400.
- ❖ Logging procedures: Two separate logs are utilized in each area:
 - Log #1: Information review and analysis only in the data storage area location where the "Master Copy" is stored. Copies should be limited, but can be re-produced and must be returned to POC prior to departing data storage area.
 - Name (Last, First, MI)
 - Non-disclosure agreement on file (yes/no), if no access is denied
 - Date (dd/mmm/yy) signed out (to work in the designated data analysis work area).
 - Time (24 hour clock)
 - Date (dd/mmm/yy) returned

- Time (24 hour clock)
 - Rank, Civilian (Title, grade)
 - Organization (Ranges workgroup)
 - Description of information
 - Purpose (why access is requested)
 - Log #2: Information copied for removal
 - Name (Last, First, MI)
 - Non-disclosure on file (yes/no) If no access is denied
 - Date (dd/mmm/yy) copied
 - Time (24 hour clock)
 - Rank, Civilian (Title, grade)
 - Organization (Ranges workgroup)
 - Number of Pages copied
 - Description of information
 - Reason for copy
 - Log #3: Access check log; Recap of Log 1 and 2 on monthly basis.
 - Date (by month)
 - Ranges Subgroup working group title
 - Data requests for analysis in designated storage area
 - Data requests to be copied/removed
 - Rank, Civilian (Title, grade)
- ❖ "Master" (original data) copies notes, or computations will not be removed from the Rm 1E121 secure area without prior approval of the E&T JCSG Ranges Subgroup working lead POC Mr. Thomas Macia 703-692-6410. Movement of original data outside the secure area is limited to the E&T JCSG Ranges Subgroup working lead POC and/or his designated alternate.
- Ensure all documents are properly marked with BRAC header/footer information (Draft Deliberative Document – For Discussion Purposes Only Do Not Release Under FOIA).
 - If personnel are authorized to leave the BRAC Controlled Data Secure Area(s) with BRAC data, the data and cover sheet will be in manila envelope and/or sufficient containers to secure information. Personnel transporting such material must have the ability to restrict access to the data at interim and final destinations. Taking data out of the secure area is the exception not the norm.
 - The use of e-mail for discussion, notes, and computations is prohibited.

4. Access Requirements:

a. Data access is limited to members of the JCSG- E&T Ranges Subgroup and to those the E&T JCSG Ranges Subgroup working lead POC Mr. Thomas Macia 703-692-6410, or Mr. John Foulkes, 703-695-8996, T&ESWG POC for T&ESWG matters, designates in accordance with sign-in procedures listed paragraph # 3. The alternate POCs will maintain a list of individuals granted access to the information within each facility/secure area. The alternate POC (Mr. Bob Lepianka and Mr. C. Buchanan, respectively) is responsible for opening and securing the data/facility. The list is modified only with the approval of the E&T JCSG Ranges Subgroup or T&ESWG POC. The alternate POCs will maintain a list of individuals who have signed a Non-Disclosure Agreement. The alternate POCs will serve as the point of contact for access and availability of data. Respective sub-working groups will work from their "Master Copy" of the data. Each primary Subgroup and sub-working group member (service designees) will have equal access to the data. However, the alternate POCs (Mr. Bob Lepianka and Mr. C. Buchanan) with concurrence from the subgroup POC, Mr. Tom Macia, or T&ESWG POC, Mr. John Foulkes, will make the determination whether varying levels of access are authorized for support members based upon the situation.

b. Additional Access Requirements:

Draft Deliberative Document – For Discussion Purposes Only
Do Not Release Under FOIA

- ❖ An access authorization list of personnel with authorized access to each facility/secure area is maintained by the respective alternate POC and checked when access is requested. Subgroups will work with their individual “Master Copy” and not the “Original Document”.
 - No access is granted if the individual is not on the approved list. Access is not granted to an individual until the individual goes through channels with appropriate documentation and approval.
 - Non-disclosure agreements are maintained as backup documentation to the approved access list.
 - One time access to data/secure area for Subject Matter Experts (SME) is granted by the E&T JCSG Ranges Subgroup working lead or T&ESWG POC. SMEs are not authorized to remove, take any of data in any form, (hard copy, notes, electronic) from the Ranges Subgroup or T&ESWG data storage areas (1E1221/3400). Subgroup or T&ESWG POC will ensure all SMEs have signed non-disclosure statements

5. Other Requirements:

a. All data, including copies/version in any form are centrally stored in each area. To prevent unauthorized access to data submissions, suite access is restricted by locking suite/steel storage containers whenever they are unattended or when not in use.

b. Other Requirements:

- ❖ SOP's will be reviewed monthly and updated as required.
- ❖ Access checks will be run monthly and logged to gage whom (by Ranges Subgroup workgroup and T&ESWG) and how often access has been requested/utilized.
- ❖ If the requirement for a Supplemental Data call arises, the collected information will be handled in the same manner as described above.
- ❖ Supplemental/Corrected data: If/when supplemental data is received it will be inserted as a replacement page to the original data file. The original data replaced will be saved in a back-up file for reference. The original hard copy: The page will be replaced with the supplement data and the original page will be shredded. (The original will be in a back up file on disk, no reason to save hard copy) Same replacements will be made to Master Hard Copy documents for Rm 1E121 and Rm 3400.

Alternate E&T JCSG Ranges Subgroup working POC is Mr. Robert Lepianka, 703-692-6427, DAMO-TRS. Alternate T&ESWG POC is Mr. C. Buchanan, 703-601-1760, N091.

BUFORD C. BLOUNT, III
Major General, GS
Assistant Deputy Chief of Staff, G-3

Addendum 1 to JCSG-Ranges ICP SOP dated 30 Jan 2004

Receipt of data call information from E&T JCSG Chiefs

- a. E&T JCSG Chiefs will provide the E&T JCSG Range subgroup with the BRAC data call information via CD. The Range alternate POC is designated the individual authorized to transport the BRAC information. While transporting BRAC information, media should be appropriately covered with "close hold" cover sheet and protected from possible disclosure.
- b. Upon arrival back at the Range work site, 1E121, Pentagon the CD will be logged according to the Range ICP SOP as per log #1. The alternate POC will copy the CD onto the Range designated computer using the C drive, BRAC file. The Range POC will verify everything was copied from the CD to the C drive, BRAC file. The CD will then be secured in accordance with Range ICP SOP. This CD will not be used again unless the file on the C Drive should become corrupt. Paper copies of the C drive BRAC information will be logged and distributed to Range members according to Range ICP SOP. The chair and POC, and alternate POC's are the only members of the subgroup who are authorized to make copies of the BRAC information. Range members are required to secure the paper copies of BRAC data according to Range ICP SOP.

Transfer of information into the subgroup analysis tool

- a. The Range alternate POC designates the Range data analyst primary Service Range member's authority to take the information off the C drive BRAC file and input it directly into the Range analysis tool. Each member is responsible for verifying the accuracy of the BRAC information entered into the tool. Range members who enter BRAC information into the tool must have another Range member verify information accuracy. The DODIG is responsible for performing spot checks on the accuracy of the BRAC data transfer. If data entry errors are discovered, the member committing the error or POC will make immediate corrections and the change revalidated for accuracy.

Receipt of supplemental data call information from E&T JCSG Chiefs

- a. E&T JCSG Chiefs will provide the E&T JCSG Range subgroup with the BRAC supplemental data call information via CD. The Range alternate POC is the designated individual authorized to transport the BRAC information. While transporting BRAC supplemental information, media transported should be appropriately covered with "close hold" cover sheet and protected from possible disclosure.
- b. Upon arrival back at the Range subgroup worksite, 1E121, Pentagon the CD will be logged according to the Range subgroup ICP SOP. The alternate POC will copy the CD onto the Range computer using the C drive, BRAC file. The supplemental information will be stored in folders on the C drive, BRAC file as follows:
 - Data Call Number
 - Army
 - Question 103 (Example)
 - Question 108 (Example)
 - Navy/Marine Corps
 - Air Force
 - Defense Agencies
 -

The Range alternate POC will verify everything was copied from the CD to the C drive, BRAC file. The CD will then be secured in accordance with Range ICP SOP. This CD will not be used again unless the file on the C drive should become corrupt. Paper copies of the C drive BRAC supplemental information will be logged and distributed to Range members according to Range

ICP SOP. The Chair, POC, and alternate POC are the only members of the subgroup who are authorized to make copies of the BRAC supplemental information. Range members are required to secure the paper copies of BRAC supplemental data according to Range ICP SOP.

c. The Range alternate POC is responsible for incorporating supplemental data into the C drive, BRAC file. The Range alternate POC will identify the specific question, data element. And response to be changed. In the electronic files (access and MS Word), the Range alternate POC will key enter updated response in the appropriate location(s) and in the MS Word add a footnote that includes the date, log number, and change. For PDF files, the Range alternate POC will attach a comment (date, log number, and change) to the specific PDF file that is being updated. A primary Service Range member will verify the supplemental data was updated correctly in the C drive, BRAC file. The DODIG is responsible for performing spot checks on the accuracy of the BRAC supplemental data transfer. If data entry errors are discovered, the POC will make immediate corrections and the change revalidated for accuracy. The alternate POC will identify to the primary Service Range member that supplemental data has been received and changes are required in the data tool.

d. The Range alternate POC designates the Range data analyst and primary Service Range member's authority to take the information off the C drive BRAC supplemental file and input it directly into the Range analysis tool. Each member is responsible for verifying the accuracy of the BRAC supplemental information entered into the tool. Range members who enter BRAC supplemental information into the tool must have another Range member verify information accuracy. The DODIG is responsible for performing spot checks on the accuracy of the BRAC supplemental data transfer. If data entry errors are discovered, the POC will make immediate corrections and the change revalidated for accuracy. The Range data analyst and primary Service Range members must review all analysis tools to determine all areas impacted by the supplemental information.

CALIBRE access requirements

a. CALIBRE will receive or send data on a CD or floppy disc to/from the E&T JCSG Range's subgroup data security POC (Mr. Bob Lepianka) from/at his Pentagon location. 1E121.

b. All work at CALIBRE headquarters (6354 Walker Lane, Metro Park, Alexandria, VA 22310-3252) will occur within secure office that will be secured 24/7. The office is room number 5019 located on the 5th floor of CALIBRE, Metro Park, Alexandria, VA.

- The secure office will allow only limited access to a predetermined list of CALIBRE employees. Employees with access have both a Secret Security clearance and have signed a Non-Disclosure Agreement. ((Non-Disclosure on file at both CALIBRE HQ and Pentagon, Rm 1E121.
- The secure office will include a sign in sheet, documenting dates and times of entrance and egress.
- The master data CD copy received from Range subgroup alternate POC will be loaded onto two secure desktop computers that will NOT be connected to the LAN and the copy of the Master will be stored in a locked storage container in the office of Ms. Amy Dubois, CALIBRE Headquarters.

Addendum 1 A

JCSG-Ranges ICP SOP dated 30 Jan 2004

25 Jun 04

Receipt of data call information from E&T JCSG Chiefs

- a. E&T JCSG Chiefs will provide the E&T JCSG Range subgroup with the BRAC data call information via CD. The Range alternate POC is designated the individual authorized to transport the BRAC information. While transporting BRAC information, media should be appropriately covered with "close hold" cover sheet and protected from possible disclosure.
- b. Upon arrival back at the Range work site, 1E121, Pentagon the CD will be logged according to the Range ICP SOP as per log #1. The alternate POC will copy the CD onto the Range designated computer using the C drive, BRAC file. The Range POC will verify everything was copied from the CD to the C drive, BRAC file. The CD will then be secured in accordance with Range ICP SOP. This CD will not be used again unless the file on the C Drive should become corrupt. Paper copies of the C drive BRAC information will be logged and distributed to Range members according to Range ICP SOP. The chair and POC, and alternate POC's are the only members of the subgroup who are authorized to make copies of the BRAC information. Range members are required to secure the paper copies of BRAC data according to Range ICP SOP.

Transfer of information into the subgroup analysis tool

- a. The Range alternate POC designates the Range data analyst primary Service Range member's authority to take the information off the C drive BRAC file and input it directly into the Range analysis tool. Each member is responsible for verifying the accuracy of the BRAC information entered into the tool. The check and balance for input accuracy is: Range members who enter BRAC information into the tool must have another Range member verify information accuracy. The DODIG is responsible for performing spot checks on the accuracy of the BRAC data transfer. If data entry errors are discovered, the member committing the error or POC will make immediate corrections and the change revalidated for accuracy.

Receipt of supplemental data call information from E&T JCSG Chiefs

- a. E&T JCSG Chiefs will provide the E&T JCSG Range subgroup with the BRAC supplemental data call information via CD. The Range alternate POC is the designated individual authorized to transport the BRAC information. While transporting BRAC supplemental information, media transported should be appropriately covered with "close hold" cover sheet and protected from possible disclosure.
- b. Upon arrival back at the Range subgroup worksite, 1E121, Pentagon the CD will be logged according to the Range subgroup ICP SOP. The alternate POC will copy the CD onto the Range computer using the C drive, BRAC file. The supplemental information will be stored in folders on the C drive, BRAC file as follows:
 - Data Call Number
 - Army
 - Question 103 (Example)
 - Question 108 (Example)
 - Navy/Marine Corps
 - Air Force
 - Defense Agencies

The Range alternate POC will verify everything was copied from the CD to the C drive, BRAC file. The CD will then be secured in accordance with Range ICP SOP. This CD will not be used again unless the file on the C drive should become corrupt. Paper copies of the C drive BRAC supplemental information will be logged and distributed to Range members according to Range ICP SOP. The Chair, POC, and alternate POC are the only members of the subgroup who are authorized to make copies of the BRAC supplemental information. Range members are required to secure the paper copies of BRAC supplemental data according to Range ICP SOP.

c. The Range alternate POC is responsible for incorporating supplemental data into the C drive, BRAC file. The Range alternate POC will identify the specific question, data element. And response to be changed. In the electronic files (access and MS Word), the Range alternate POC will key enter updated response in the appropriate location(s) and in the MS Word add a footnote that includes the date, log number, and change. For PDF files, the Range alternate POC will attach a comment (date, log number, and change) to the specific PDF file that is being updated. A primary Service Range member will verify the supplemental data was updated correctly in the C drive, BRAC file. The DODIG is responsible for performing spot checks on the accuracy of the BRAC supplemental data transfer. If data entry errors are discovered, the POC will make immediate corrections and the change revalidated for accuracy. The alternate POC will identify to the primary Service Range member that supplemental data has been received and changes are required in the data tool.

d. The Range alternate POC designates the Range data analyst and primary Service Range member's authority to take the information off the C drive BRAC supplemental file and input it directly into the Range analysis tool. Each member is responsible for verifying the accuracy of the BRAC supplemental information entered into the tool. Range members who enter BRAC supplemental information into the tool must have another Range member verify information accuracy. The DODIG is responsible for performing spot checks on the accuracy of the BRAC supplemental data transfer. If data entry errors are discovered, the POC will make immediate corrections and the change revalidated for accuracy. The Range data analyst and primary Service Range members must review all analysis tools to determine all areas impacted by the supplemental information.

CALIBRE access requirements

a. CALIBRE will receive or send data on a CD or floppy disc to/from the E&T JCSG Range's subgroup data security POC (Mr. Bob Lepianka) from/at his Pentagon location. 1E121.

b. All work at CALIBRE headquarters (6354 Walker Lane, Metro Park, Alexandria, VA 22310-3252) will occur within secure office that will be secured 24/7. The office is room number 5019 located on the 5th floor of CALIBRE, Metro Park, Alexandria, VA.

- The secure office will allow only limited access to a predetermined list of CALIBRE employees. An employee's access roster will be posted on the entrance door to the secure room. Employees with access have both a Secret Security clearance and have signed a Non-Disclosure Agreement. ((Non-Disclosure on file at both CALIBRE HQ and Pentagon, Rm 1E121.
- The secure office will include a sign in sheet, documenting dates and times of entrance and egress.
- The master data CD copy received from Range subgroup alternate POC will be loaded onto one secure desktop computer that will NOT be connected to the LAN and the copy of the Master CD will be stored in a locked storage container in the office of Ms. Amy Dubois, CALIBRE Headquarters.

E&T JCSG-Ranges ICP SOP dated 30 Jan 2004 Capacity Analysis Clarification Process/Procedure

1. PURPOSE

This document outlines the procedures for E&T JCSG members to request from the various Department of Defense entities and Branches of Services clarification concerning the BRAC 2005 Capacity and Military Value questions. The intent of this effort is to address current questions and answers of Data Call #1. Obtaining correct data to the current "as is" capacity questions is the objective. Seeking supplemental capacity related data is not the intent. Supplemental capacity data requests require separate data calls with short turn suspense's.

2. REFERENCES

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.*

- Defense Base Closure and Realignment Act of 1990 (Public Law 101-510, as amended).
- Memorandum, Secretary of Defense, 15 November 2002, Subject: Transformation Through Base Realignment and Closure.
- Message, Secretary of Defense, 13 February 2003, Subject: Public Affairs Guidance (PAG) – Transformation Through Base Realignment and Closure (BRAC 2005).
- Message, Secretary of Defense, 20 November 2003, Subject: Public Affairs Guidance (PAG) – Transformation Through Base Realignment and Closure (BRAC 2005).

Email Message, McAndrew, Michael, Mr, OSD-ATL, 6 May 2004, Subject: Data Call #1 Clarification (Note: addresses coordination points of contacts for resolving incomplete or erroneous information)

3. CLARIFICATION PROCESS

The following procedures outline the steps to request clarification for incomplete, unclear, erroneous and or unanswered information:

E&T JCSG staff and/or Subgroup

- Identify requirement, establish a data delivery due date, document requests using the E&T JCSG tracking tool (must be auditable), and assign category to requirement as follows:
- Missing Data: Data is incomplete or missing
- Erroneous Data: Data appears to be inaccurate or is inconsistent with responses from other MILDEPS, agencies, and activities.
- MILDEP Tool Problem: The limitations of a specific MILDEP data collection tool are creating a situation where the data is not recognizable, translatable or understandable.
- Structural Issue: Problems/issues with the Master Database (will be directed to OSD BRAC)

Forward the request for information to the appropriate E&T JCSG Service BRAC Representatives identified below:

- Air Force: Send all inquires to AF BRAC Help Desk via E-Mail to af.brachelpdesk@pentagon.af.mil. The lead O-6/GS-15 of the JCSG or of a JCSG Subgroup is to provide the initial tasking e-mail to the Help Desk. The Help Desk is responsible for reviewing, coordinating, tracking, and changing the data through established adjudication process. The SAF/IEBB Helpdesk Personnel contacts include:

- Mr Martin Bullock, 692-5122
 - Mr Bob Tuck: 692-5123
 - Ms Paula Loomis: 692-9514
 - Mr Chuck Meshako: 692-5124
 - Mr Roy Murray: 692-5121
 - Army: Mr. Bob Harrison, 703-692-7780, robert.harrison@us.army.mil
 - Navy: Capt Gene Summerlin, 703-602-6431, gene.summerlin@navy.mil
 - Flight Training subgroup: Capt Gene Summerlin, 703-602-6431, gene.summerlin@navy.mil
 - Ranges subgroup: CDR Joe Arleth, 703-602-6436, joseph.arleth@navy.mil
 - Specialized Skills and Training subgroup: CDR Greg Hilscher, 703-602-6433, greg.hilscher@navy.mil
 - Professional Development and Education subgroup: LtCol Mark Murphy, 703-602-6438, mark.murphy2@navy.mil
- Monitor all Open Requests on a regular basis with the “Open Clarification Report”. Coordinate all “Past Due Requests” needing escalation with Service BRAC representatives and E&T JCSG Coordination Team. E&T JCSG Coordination Team will submit request for assistance to the BRAC office and/or E&T JCSG Service Principles. If issues raised by your Service Principal cannot be resolved by a particular Military Department, they will be forwarded to the ISG for adjudication.
- Close Clarification Request in the E&T JCSG tracking tool upon receiving a confirmation that the certified data has been incorporated into the OSD JCSG Master Production Capacity Analysis Database.
- Service BRAC Representatives
 - The Service BRAC representatives are the central point of contact for the E&T JCSG sub-groups to monitor the status of all requests to their various entities.
 - Ensures requests for clarification are forwarded to the appropriate unit/organization.
 - Ensures the unit/organization data is certified and captured by the established delivery suspense date.
 - Ensures the certified data is captured into Service data tool and OSD BRAC or forwarded to the E&T JCSG through approved procedures.
- OSD BRAC
 - Captures the certified data from the various DoD and Services databases and post updates at least weekly to the JCSG Master Database.
 - Notifies the JCSG when changes to the OSD Master Database are available for updating the JCSG Production sources.
- E&T JCSG Coordination Team
 - Updates the certified changes to the E&T JCSG Production database.
 - Notifies the E&T JCSG sub-groups when changes are available and ready for use.

**E&T JCSG-Ranges ICP SOP dated 30 Jan 2004; Addendum 1
Receipt of supplemental data call information subpara c.**

1. Addendum 3 supercedes addendum 1 paragraph c.
2. Paragraph now reads: The Range alternate POC is responsible for incorporating supplemental data on to the desktop as an access database file. The file will be labeled "E&T BRAC analysis Data Base (Then the current number #), the old data base will be moved to the JCSG desktop folder, and file under old information. No more than the past two databases will be kept in the old file. The hard drive is removable. It is removed nightly and secured as per SOP instructions. All of the old databases will be stored in a secure cabinet on cd for reference and audits. Each database comes with a hard copy print out of the question numbers that were changed and the installations that changed them.
 - The Range alternate POC will identify the specific questions (questions specifically used by the Training subgroup for capacity analysis and questions that were sent as requests for clarification. The alternate POC will create a data base cd and copy of the hard copy question printout for the T&E to sign for and receive. T&E will be responsible for handling the supplemental data as per T&E specific ICP SOP instructions.
 - Range Training has no supplemental data but does have requests for clarifications. These specific question numbers are:
 - Ground training: #152, 157
 - Air: #160, 169
 - Sea: #192, 193
 - Data updates will be implemented as follows:
 - Data questions will be queried and saved as an excel file for use in updating.
 - Data in excel will be identified by target location and question.
 - Data will be updated on the master excel capacity analysis spreadsheet for training.
 - The master spreadsheet will be annotated in the installation name box by the last data base number that was updated. (db3).
 - The hard copy printout will be annotated and filed. The filed hard copy will be the audit trail for the execution of the data base updates.
 - A primary Service Range member will verify the supplemental data was updated correctly in the C drive, BRAC file. The DODIG is responsible for performing spot checks on the accuracy of the BRAC supplemental data transfer. If data entry errors are discovered, the POC will make immediate corrections and the change revalidated for accuracy. The alternate POC will identify to the primary Service Range member that supplemental data has been received and changes are required in the data tool.

E&T JCSG-Ranges ICP SOP dated 30 Jan 2004; Addendum 1**Safeguard procedures for the use to OSD TJCSG Secure Portal for information and data transfer.**

Portal Access Control Roster: POC for portal access for the training subgroup is Mr. Robert S. Lepianka, POC for T&E is Mr. Roy Owens.

- Training Access Roster
 - Mr Robert Lepianka POC
 - Mr. Thomas Macia Range Subgroup POC
 - CDR Joseph Arleth Sea domain USN
 - LCDR Kristina Nielsen Sea domain USN
 - Mr James Sample Air domain USAF
 - Ms. Kerry Sawyer Grd domain USMC
 - LtCol Wren Meyers Grd domain USMC
 - Mr. Markus Craig Calibre Systems
 - MAJ Michael Hitchcock JFCOM
 - Mr Robert Harrison Army Liaison TABs
- T&E Access Roster
 - Mr Roy Owens POC
 - Dr John Folkes T&E Subgroup POC
 - Beth Schaeffer DoD IG
 - Mr Thomas Dobry USAF
 - Mr Dan Long USN
 - MAJ Martin Whalen USAF
 - Mr Paul Schaeffer USAF
 - Mr Skip Buchanan USN
 - Mr Irv Boyles DO T&E
 - Mr Ray Fontaine USA

E&T JCSG-Ranges ICP SOP dated 22 Feb 2005**Range Subgroup SOP Update for Safeguarding Base Realignment and Closure (BRAC) Data.**

Addendum 5 change 1: **Storage Requirements:** Store data in DAMO-TRS Rm 1E121, Pentagon, Arlington Virginia for use by the Training sub-working groups is

Change to: Store data in Rosslyn Office, 1401 Wilson Blvd., Rosslyn, VA, 22209-2325, 5th floor suite 501 Range Subgroup office, room number 551. All data storage and accounting requirements remain static.

Addendum 5 change 2: It is the responsibility of Mr. John Foulkes, 703-695-8996, to inform N091 administration of the departure or addition of any permanent T&ESWG member.

Change to: It is the responsibility of Mr Brian Simmons, 410-278-1016, to inform N091 administration of the departure or addition of any permanent T&ESWG member.

Addendum 5 change 3: Administrative Functions conducted at the Pentagon 1E121.

Change to: All administrative functions conducted at the Pentagon, 1E121 will remain the same, except they will now be conducted in Rosslyn.

Addendum 5 change 4: Control requirements paragraph 3 sub-paragraph a & b; conducted at the Pentagon, 1E121.

Change to: All control requirements conducted at the Pentagon, 1E121 will remain the same, except they will now be conducted in Rosslyn.

Addendum 5 change 5: Access requirements paragraph 4 sub-paragraph a; Data access is limited to members of the JCSG- E&T Ranges Subgroup and to those the E&T JCSG Ranges Subgroup working lead POC Mr. Thomas Macia 703-692-6410, or Mr. John Foulkes, 703-695-8996, T&ESWG POC for T&ESWG matters.

Change to: Access requirements paragraph 4 sub-paragraph a; Data access is limited to members of the JCSG- E&T Ranges Subgroup and to those the E&T JCSG Ranges Subgroup working lead POC Mr. Thomas Macia 703-692-6410, or Mr Brian Simmons, 410-278-1016, T&ESWG POC for T&ESWG matters.

Addendum 5 change 6: Access requirements paragraph 4 sub-paragraph a; Each primary Subgroup and sub-working group member (service designees) will have equal access to the data. However, the alternate POCs (Mr. Bob Lepianka and Mr. C. Buchanan) with concurrence from the subgroup POC, Mr. Tom Macia, or T&ESWG POC, Mr. John Foulkes, will make the determination whether varying levels of access are authorized for support members based upon the situation.

Change to: Access requirements paragraph 4 sub-paragraph a; Each primary Subgroup and sub-working group member (service designees) will have equal access to the data. However, the alternate POCs (Mr. Bob Lepianka and Mr. C. Buchanan) with concurrence from the subgroup POC, Mr. Tom Macia, or T&ESWG POC, Mr. Brian Simmons, will make the determination whether varying levels of access are authorized for support members based upon the situation.

Change to: All of the rest of the access requirements conducted at the Pentagon, 1E121 will remain the same, except they will now be conducted in Rosslyn.

Addendum 5 change 7: Other requirements paragraph 5 sub-paragraph a and b;

Change to: All of the rest of the other requirements conducted at the Pentagon, 1E121 will remain the same, except they will now be conducted in Rosslyn.

Addendum 5 change 1 to addendum 1: Receipt of data call information from E&T JCSG chiefs, sub-paragraph a and b.

Change to: All of the rest of the receipt of data information from E&T JCSG chiefs conducted at the Pentagon, 1E121 will remain the same, except they will now be conducted in Rosslyn.

Addendum 5 change 2 to addendum 1: Transfer of information into the subgroup analysis tool, sub-paragraph a, The Range alternate POC designates the Range data analyst primary Service Range member's authority to take the information off the C drive BRAC file and input it directly into the Range analysis tool. Each member is responsible for verifying the accuracy of the BRAC information entered into the tool. The check and balance for input accuracy is: Range members who enter BRAC information into the tool must have another Range member verify information accuracy. The DODIG is responsible for performing spot checks on the accuracy of the BRAC data transfer. If data entry errors are discovered, the member committing the error or POC will make immediate corrections and the change revalidated for accuracy.

Change to: The Range alternate POC designates the Range data analyst primary Service Range member's authority to take the information off the CAD and MAD E&T JCSG data CDs and input them directly into the Range analysis tool for capacity. Data for Mil Val is copied from the original data cd, logged out and signed for by the POC (Mr. Karl Kalb) to Calibre Systems. Calibre Systems, in turn merges the raw MIL Val data into the Mil Val data bases for analysis.

Change to: The DODIG is responsible for performing spot checks on the accuracy of the BRAC data transfer. If data entry errors are discovered, the member committing the error or POC will make immediate corrections and the change revalidated for accuracy. Spot checks are not conducted but rather a full DoD IG validation of the capacity and mil val output. Any discrepancies are returned to the Subgroup POC via DoD IG memo, with a S: for documented corrections. The same procedures hold for Mil Val, except the POC is Mr KARL Kalb at Calibre.

Addendum 5 change 3 to addendum 1: Receipt of supplemental data call information from E&T JCSG chiefs sub-paragraphs a,b,c,and d.

Change to: All of the rest of the receipt of supplemental data call information from E&T JCSG chiefs conducted at the Pentagon, 1E121 will remain the same, except they will now be conducted in Rosslyn.

Addendum 5 change 4 to addendum 1: Calibre access requirements sub-paragraph a and b. all references to 1E121.

Change to: Rosslyn location

Change to: Replace Amy Dubois with Chuck Fowler

Addendum 5 change 1 to addendum 1A: All references to Pentagon, 1E121

Change to: Rosslyn location.

Addendum 5 change 1 to addendum 4: Portal access control roster.

Change to: T&E access roster Replace Dr. John Folks with Mr Brian Simmons

Addendum 5 addition 1 Range Subgroup SOP: Key Points of Contact, Each subgroup is responsible for providing adequate controls and management oversight to protect against the release of subgroup's information to unauthorized personnel. The Range Subgroup key points of contact are:

- | | | |
|-----------------------------------|---------------------|----------------------|
| • Range Subgroup POC: | Mr Thomas Macia | 703-692-6417 |
| • Range Subgroup T&E POC: | Mr. Brian Simmons | 410-278-1016 |
| • Range Subgroup Tng Sr. Analyst: | Mr. Robert Lepianka | 703-696-6435 ext 288 |
| • Range Subgroup T&E Alt POC: | Mr Ray Fontaine | 410-278-1025 |
| • Range Subgroup T&E Sr. Analyst: | Mr Roy Owens | 763-998-1691 |
| • Range Subgroup Tng Air: | COL James Wilson | 703-588-6369 |
| • Range Subgroup Tng Sea: | CDR Joseph Arleth | 703-602-6436 |
| • Range Subgroup Tng Grd: | LtCol Wren Myers | 703-432-1248 |

Addendum 5 addition 2 Range Subgroup SOP: Administrative responsibilities add paragraph c: Information disclosure. Everyone involved in the BRAC 2005 process must use every precaution to prevent 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, car must also be taken to avoid inadvertent dissemination of such information through verbal conversation, facsimile, e-mail, or other electronic communication means.

Addendum 5 addition 3 Range Subgroup SOP: Access requirements add paragraph c. Information access; Access to copies of deliberative and/or draft deliberative documents will be restricted to those individuals who have signed Non-disclosure Agreements that are on file in Suite 502 and on a need to know basis. All deliberative documents are "CLOSE HOLD" information and shall be maintained in the Range Subgroup secure office space. Authorized individuals who remove copies of deliberative and/or draft deliberative documents (electronic or paper) from Range Subgroup secure office space must first obtain permission from the Range Subgroup POC or Senior Analyst and sign for the material in a sign-out log maintained by the Range Subgroup senior analyst. The following is a quote from Policy Memorandum One, referenced above.

Addendum 5 addition 4 Range Subgroup SOP: Control requirements; add paragraphs for "Document Destruction", and "Information Security Breach".

- Document Destruction: As required, BRAC documents will be returned to the Range Subgroup senior analysts for disposition. It is each person's responsibility to ensure all other BRAC related documents not under document control are placed into the burn bags. The DoD Incinerator organization is responsible for destroying classified and unclassified documents, IAW Administrative Instruction 26, Chapter 9.
- Information Security Breach: All precautions must be taken to avoid loss/unauthorized release of "CLOSE HOLD" information that is considered or produced by the Range Subgroup. Attention to detail and training are the best preventative measures to avoid a security breach. However, if and when a security breach incident occurs, the following checklist shall be used:

The individual identifying the breach shall:

1. Conduct an immediate search of the local area and question personnel in the vicinity.
2. Notify the Range subgroup POC or the alternate (senior analyst).

The Alternate POC:

1. Conduct an exhaustive search in the vicinity of the document's/CD's last known location.
2. Assess the nature/impact of the loss/unauthorized release of the "CLOSE HOLD" information.
3. Report incident status to the E&T JCSG Chief.

The E&T JCSG Chair Persons shall:

1. Review the incident.
2. Expand the search/open an investigation concerning the incident, as seen fit.
3. Assess potential damage/publicity that could be associated with the incident.
4. At their discretion, inform all appropriate authorities of the nature, extent, and resolution of the security breach.

Addendum 5 addition 5 Range Subgroup SOP: Control requirements; add paragraphs for "Facsimile usage;

The use of facsimile machines to transmit information such as Military Value Scoring Plans, data call questions and responses, scenarios, possible alternatives, or recommendation candidates is not permitted. Information not dealing with Military Value Scoring Plans, data call questions and responses, scenarios, possible alternatives, or recommendations may be faxed to authorized recipients. Individuals are responsible for logging in the appropriate information into the "Document Fax Log". Care will be taken to ensure that the facsimile machine is monitored during transmission and receipt to preclude any compromise of sensitive information. The procedure is that contact between the individuals sending/receiving the fax must be made and that each individual must be present at the FAX to control

transferred documents and confirm receipt. A sign will be posted on the facsimile machine stating the requirement for monitoring transmissions. This is not the normal means of communication.

Addendum 5 addition 6 Range Subgroup SOP: Control requirements; add paragraph Facsimile Log. Log number 6.

- Log #6: Information faxed
 - Name (Last, First, MI)
 - Non-disclosure on file (yes/no) If no access is denied
 - Date (dd/mmm/yy) copied
 - Time (24 hour clock)
 - Rank, Civilian (Title, grade)
 - Organization (Ranges workgroup)
 - Number of Pages faxed
 - Description of information
 - Reason for fax