

**Transformation through  
Base Realignment and Closure  
Technical Joint Cross Service Group  
Information Control Procedures**

**April 13, 2004**

DRAFT DELIBERATIVE DOCUMENT-FOR DISCUSSION ONLY - DO NOT RELEASE UNDER FOIA

BRAC FOUO

TECHNICAL JOINT CROSS-SERVICE GROUP (TJCSG)  
BASE REALIGNMENT AND CLOSURE (BRAC) 2005  
INFORMATION CONTROL PROCEDURES

Table of Contents:

1.	Introduction.....	4
2.	Purpose.....	4
3.	References.....	4
4.	Policy Guidance.....	5
5.	Responsibilities.....	5
6.	BRAC Data:.....	6
6.1.	Classified Data:.....	6
6.2.	Sensitive Data.....	6
7.	Storage Requirements.....	6
7.1.	Physical location used to store data.....	6
7.2.	Type of container(s) used to store data.....	6
7.3.	Information Technology Containers.....	7
8.	Office Space Security.....	7
8.1.	TJCSG Office Spaces.....	7
8.2.	Physical Security at the Crystal City Location.....	7
8.3.	Physical Security at the Rosslyn Location.....	7
8.4.	Office Visitors.....	7
8.5.	Use of Wireless Devices.....	8
8.6.	Individual Office Spaces.....	8
9.	Document Control.....	8
9.1.	TJCSG Working Papers and Documents.....	8
9.2.	BRAC Certified Data.....	8
9.3.	TJCSG Generated Data/Documents.....	8
9.4.	Information Access.....	8
9.5.	Removal of BRAC Data from Secure Office Space.....	8
9.6.	Performing Analysis.....	8
10.	Use of Facsimile.....	9
10.1.	General Use.....	9
10.2.	Restrictions.....	9
11.	Use of Telephone.....	9
11.1.	One-on-one Phone Conversation.....	9
11.2.	Use of Speakerphones.....	9
11.3.	Teleconferences.....	9
12.	Use of E-mail.....	9
12.1.	SIPRNET.....	9
12.2.	Unclassified Network.....	10
12.3.	Precautions.....	10
12.4.	Use of Web Portal.....	10
12.4.1.	Introduction (and intended use).....	10
12.4.2.	Portal Requirements Document.....	10

DRAFT DELIBERATIVE DOCUMENT-FOR DISCUSSION ONLY – DO NOT RELEASE UNDER FOIA

BRAC FOUO

12.4.3. Access to Portal..... 10  
12.4.3.1 Restricted Portal Access ..... 10  
12.4.3.1 Open Access to Portal ..... 10  
12.4.4. Configuration Management..... 10  
12.4.5. Content Data Management..... 10  
13. Computer Security..... 11  
13.1. Safeguarding the Computers..... 11  
13.2. Transporting Data Storage Devices ..... 11  
14. Meeting Minutes and Record Keeping..... 11  
14.1. TJCSG Meeting Minutes ..... 11  
14.2. CIT Meeting Minutes..... 11  
14.3. Subgroup Meeting Minutes..... 11  
14.4. Records Keeping..... 11  
15. Open Source Data..... 12  
16. Office Procedures for Correspondence..... 12  
17. Updating the Document..... 12  
18. Continuity of Operations Planning (COOP)..... 13  
19. Plan end Date ..... 13  
20. Closing Remark..... 13  
  
APPENDIX A Acronyms ..... 15  
  
APPENDIX B Risk Assessment..... 16  
  
APPENDIX C Security Procedures for the TJCSG Office Spaces Located at Crystal City ..... 17  
  
APPENDIX E: CLOSE HOLD Cover Page..... 25  
  
APPENDIX F: List of Authorized Individuals to Transport Sensitive BRAC DATA..... 27

DRAFT DELIBERATIVE DOCUMENT-FOR DISCUSSION ONLY – DO NOT RELEASE UNDER FOIA

**TECHNICAL JOINT CROSS-SERVICE GROUP (TJCSG)  
BASE REALIGNMENT AND CLOSURE (BRAC) 2005  
INFORMATION CONTROL PROCEDURES**

**1. Introduction.**

The BRAC 2005 process is designed to provide a structured and systematic approach for developing base realignment and closure recommendations for submittal to the Commission in May 2005. Throughout the process, all military installations are considered equally, without regard to prior consideration for realignment or closure. The base realignment and closure recommendations resulting from this process will be based on the force structure plan, infrastructure inventory, and selection criteria.

The objective of the information control procedures is to employ a mechanisms that ensures the accuracy, completeness, and integrity of the information upon which the Secretary of Defense recommendations for base realignments and closures will be based. The responsibilities assigned by this document are designed to provide an “unbroken chain” of accountability for each sub-element of information used by the TJCSG in the BRAC process. Content of the document is summarized in the figure below.

<ul style="list-style-type: none"><li>▪ Policies</li><li>▪ Responsibilities</li><li>▪ BRAC Data</li><li>▪ Storage</li> <li>▪ Communication</li></ul>	<ul style="list-style-type: none"><li>▪ Record keeping</li><li>▪ Use of electronic devises</li><li>▪ Security</li><li>▪ Safeguarding BRAC Information</li></ul>
--	---

**2. Purpose.**

The primary objective of this document is to provide procedures related to controlling and safeguarding the TJCSG BRAC 2005 deliberative data, documents, decisions, and recommendations.

**3. References.**

- 3.1. Memorandum, Under Secretary of Defense (Acquisition, Technology, and Logistics), 16 April 2003, subject: Transformation through Base Realignment and Closure (BRAC 2005) Policy Memorandum One – Policy, Responsibilities, and Procedures. Includes Appendix B, Office of the Secretary of Defense Internal Control Plan for the 2005 Base Realignment and Closure Process.
- 3.2. Transformation through Base Realignment and Closure Technical Joint Cross Service Group Master Plan, dated 02 March 2004, version 1.562.
- 3.3. Base Realignment and Closure 2005 (BRAC 05), Technical Joint Cross Service Analysis Plan, Version 1.1 as of 26 March 04.

DRAFT DELIBERATIVE DOCUMENT-FOR DISCUSSION ONLY – DO NOT RELEASE UNDER FOIA

## BRAC FOUO

### 4. Policy Guidance.

- 4.1. The following is a quote from Policy Memorandum One, referenced above in paragraph 2.1. "To protect the integrity of the BRAC 2005 process, all files, data and materials relating to that process are deemed deliberative and internal to DOD. All requests for release of BRAC 2005 data and materials, including those under the Freedom of Information Act, received prior to the Secretary forwarding his realignment and closure recommendations to the Commission shall be forwarded to the DUSD(I&E)." Everyone involved in the BRAC 2005 effort must use every precaution to prevent the improper release of, or access to, BRAC 2005 information.
- 4.2. A detailed guidance and code of conducts for the TJCSG members and associates can be found in the document referenced in the paragraph 3.2.
- 4.3. Public Affairs Guidance (PAG).
  - 4.3.1. This guidance supplements the OSD PAG dated 13 February 2003, subject: Public Affairs Guidance (PAG) – Transformation through Base Realignment and Closure (BRAC 2005). The TJCSG subgroup leads will take all press, public, or Congressional inquiries without comment and forward with proposed answers to the TJCSG CIT chairman. Forwarded inquiries should include the publication name, reporter's name, and deadline.
  - 4.3.2. 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.
  - 4.3.3. The TJCSG CIT chairman will forward Congressional inquiries to OSD Legislative Affairs for response.

### 5. Responsibilities.

- 5.1. 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. The CIT and subgroup leads will ensure that the procedures listed in this document are followed.
- 5.2. It is each individual's responsibility to ensure that their desk is cleared of deliberative papers, their trash receptacles contain no BRAC papers, and that they are logged off of their PCs before leaving their permanent or temporary work areas.

DRAFT DELIBERATIVE DOCUMENT-FOR DISCUSSION ONLY – DO NOT RELEASE UNDER FOIA

## 6. BRAC Data:

### 6.1. Classified Data:

It is not anticipated that the classified material will be generated by the TJCSG. However, the TJCSG may receive classified information from the Intelligence Joint Cross Service Group or other Joint Cross Service Groups.

### 6.2. Sensitive Data.

For the purpose of this document sensitive data includes but not limited to any working or deliberative papers dealing with scenarios, possible alternatives, or recommendation candidates; documents, or electronic media containing Capacity data (raw or reduced); Military value data (raw or reduced); documents containing MV weights; Scenario data (of any type); Input or results of Optimization model runs; Input or results of COBRA runs; Any BRAC data containing location or "facility" information.

- TJCSG pre-decisional information
- Approved Equations
- Approved Weights
- Agency-organization data call responses
- BRAC decision alternatives
- TJCSG realignment and closure recommendations
- Analysis Frameworks development
- Analytical Approach
- Capacity Report
- Capacity Analysis
- Military Value Analysis
- Scenario Development and Data Call
- Cost Analysis (COBRA)
- Recommendations to Commission

TABLE- 1 TJCSG Data Items

## 7. Storage Requirements.

### 7.1. Physical location used to store data.

All TJCSG BRAC 2005 data classified and/or deemed sensitive will be stored at the TJCSG office space at Presidential Tower, 2511 Jefferson-Davis Hwy (Suite 2200) Arlington, Virginia 22202.

### 7.2. Type of container(s) used to store data.

Special containers behind locked doors with restricted access are not required, however, GSA approved containers are available at the location to secure materials up to SECRET.

### 7.3. Information Technology Containers.

The computers and networks used at the TJCSG office space are connected through dot mil server and are password protected. The necessary system administrators and the TJCSG staff will have access to the server. System Administrators will perform periodic log reviews to ensure no unauthorized access. Electronic, deliberative information such as analysis will be backed up weekly or on as needed basis on a CD and stored at the secured location. The Security Administrator will conduct weekly reviews to ensure that there are no unauthorized accesses and provide results to the CIT chair.

## 8. Office Space Security.

### 8.1. TJCSG Office Spaces.

The following office spaces are identified as primary and alternate locations for discussion and conduct of TJCSG related activities:

**8.1.1. Crystal City Office Space.** 2511 Jefferson-Davis Hwy (Suite 2200)  
Arlington, Virginia 22202

**8.1.2. Rosslyn Office Space.** 1401 Wilson Boulevard, Suite 500, Arlington,  
Virginia 22209.

**8.1.3. The TJCSG Chair office.** Room 3E1014, Pentagon

**8.1.4. The CIT Chair office.** Room 3D1089, Pentagon

**8.2. Physical Security at the Crystal City Location.** The entrance to the TJCSG office space located at the Crystal City is secured by both certified combination lock and cipher lock. The doors will remain closed and locked at all times. A security check will be conducted daily and the last designated person to leave the office will fill out a security checklist. It is each individual's responsibility to ensure each evening before leaving that their desk is cleared of deliberative papers, their trash receptacles contain no BRAC papers, and that they are logged off of their PCs. Detailed site security procedures are listed in the appendix C.

**8.3. Physical Security at the Rosslyn Location.** The Rosslyn office spaces are provided by the OSD BRAC Office. Other JCSG members are also co-located in this office spaces. The entrance to the Rosslyn office space is secured by a lock on the main access door. Electronic access is via badges that are issued and controlled by the Building Office Manager. There is a clean desk policy requiring JCSG members to ensure that prior to leaving for the day, all controlled documents are returned to the storage cabinet, desks are cleared of sensitive information, and the individuals are properly logged off of their computer.

**8.4. Office Visitors.** Visitors other than members of the TJCSG will be escorted at all times while they are in the designated secured area.

## BRAC FOUO

**8.5. Use of Wireless Devices.** Cell phones are permitted in designated office spaces as long as they cannot transmit pictures. Personal Digital Assistants (PDAs) are also allowed if they are not capable of transmitting data.

**8.6. Individual Office Spaces.** The TJCSG members working from their individual office must follow the guidance in this document and be cautious in handling the BRAC sensitive information. It is each individual's responsibility to ensure that their desk is cleared of BRAC sensitive information, and their trash receptacles contain no BRAC papers.

### 9. Document Control.

**9.1. TJCSG Working Papers and Documents.** The TJCSG and subgroup working papers and documents are generally classified as "For Official Use Only" and will contain appropriate document markings.

**9.2. BRAC Certified Data.** The certified data received from the OSD BRAC office on a hard/paper copy and/or on electronic media will be logged in and assigned a control number. For the quality assurance purposes, the original copies will remain at the secure office space under the possession of the designated security officer. The analysis team will perform their analysis from a copy of the original.

**9.3. TJCSG Generated Data/Documents.** Deliberative documents generated by the TJCSG (e.g., information dealing with scenarios, possible alternatives, or recommendation candidates) will be assigned control numbers by the TJCSG administrative staff. TJCSG administrative staff will maintain a document log containing the control number, copy number (copy 1 of N copies if applicable), title and type of document, subject, date, who accessed the data, when returned and destroyed.

**9.4. Information Access.** Access to deliberative or draft deliberative documents and other materials will be restricted to those individuals who have signed non-disclosure agreements that are on file with TJCSG or the OSD BRAC office. Signing a non-disclosure agreement does not guarantee access to all the TJCSG BRAC 05 data and/or information. Information will be provided on a need to know basis only and determination by the TJCSG chairman or the TJCSG Capabilities Integration Team (CIT) chairman. Deliberative documents will be treated as CLOSE HOLD and maintained in the TJCSG secure office space. A copy of cover CLOSE HOLD page is at Appendix E. The TJCSG administrative staff will generate a roster containing the list of individuals and the list of information they are authorized to have need and access for. This list will be used by the designated Security officer for data access control.

**9.5. Removal of BRAC Data from Secure Office Space.** Any request for removal of TJCSG BRAC related sensitive data or information dealing with scenarios, possible alternatives, or recommendations out of designated storage space will be granted on an exceptional case-by-case basis and approved by the CIT chair.

**9.6. Performing Analysis.** The designated joint analytical team supporting the TJCSG will make every effort to conduct all analyses at the designated TJCSG secured

DRAFT DELIBERATIVE DOCUMENT-FOR DISCUSSION ONLY – DO NOT RELEASE UNDER FOIA

## BRAC FOUO

office space located at the Crystal City. However, there are situations where software licensing agreements and equipment issues will prevent this from happening. Examples are use of cartographic, simulation, and optimization software or the TJCSG's lack of computing hardware. In these instances, electronic copies of data and paper copies of supporting documents will be hand carried to the analyst's parent organization, e.g., CNA. The TJCSG Chairman or the CIT Chairman will approve the temporary removal of these items on a case-by-case basis. Details of the analysis are listed in the document referenced in paragraph 3.4.

### 10. Use of Facsimile.

- 10.1. **General Use.** Facsimile can be used during questions development, reviewing draft minutes, and other information that does not include BRAC sensitive material. Care must be taken to ensure that a trusted agent monitors the facsimile machines during transmission. All facsimiles will contain appropriate BRAC security markings as described in the paragraph 16.
- 10.2. **Restrictions.** The use of facsimile machines to transmit information dealing with scenarios, possible alternatives, or recommendation candidates is prohibited at all time.

### 11. Use of Telephone.

- 11.1. **One-on-one Phone Conversation.** The TJCSG members can use telephone to discuss the BRAC sensitive on a one-on-one basis. However, a care must be taken to ensure that no one is eaves dropping into the conversation.
- 11.2. **Use of Speakerphones.** The TJCSG members are allowed to use the speakerphones in individual rooms and behind closed doors. Only authorized individuals must be allowed to listen into conversation and should be present in the room. Use of speakerphone is prohibited in an open room or exposed areas.
- 11.3. **Teleconferences.** The use of telephones for teleconferences to discuss sensitive data or information dealing with scoring plans, weights, scenarios, possible alternatives, or recommendation candidates is not permitted. Information not dealing with sensitive data or scoring plans, weights, scenarios, possible alternatives, or recommendations may be discussed over telephone. Care will be taken to ensure as to how many lines should be opened up and how many members will participate into a teleconference. A password will be provided to the members in order to join the teleconference and will be required to identify them upon joining the teleconference.

### 12. Use of E-mail.

- 12.1. **SIPRNET.** Use of unclassified e-mail to transmit information that deals with scenarios, possible alternatives or recommendations is prohibited. However, use of SIPRNET may be permitted on a case-by-case basis and upon determination by TJCSG Chairman or CIT Chairman to transmit this information point-to-point.

DRAFT DELIBERATIVE DOCUMENT-FOR DISCUSSION ONLY – DO NOT RELEASE UNDER FOIA

## BRAC FOUO

**12.2. Unclassified Network.** Use of unclassified e-mail is permitted from a dot mil to a dot mil server for questions development, reviewing draft minutes, and other information that does not deal with weights, scenarios, possible alternatives or recommendations.

**12.3. Precautions.** Communication through e-mail will contain BRAC FOUO Information in the subject line and the following information in the message body as 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.

**12.4. Use of Web Portal.**

**12.4.1. Introduction (and intended use).**

The TJCSG web portal is the principal means to exchange information among TJCSG members and associates.

**12.4.2. Portal Requirements Document**

The TJCSG Portal Requirements Document will be published separately and describe portal capabilities.

**12.4.3. Access to Portal**

Access to the TJCSG portal will be limited to the TJCSG members and associates

**12.4.3.1 Restricted Portal Access**

TJCSG members and associates are assigned access rights to portal to stored information that is deemed sensitive. An information access roster will be published and maintained separately from this document.

**12.4.3.1 Open Access to Portal**

TJCSG members and associates will have open access to planning information and information associated with their assigned mission.

**12.4.4. Configuration Management.**

The TJCSG CIT will advise of the TJCSG sub-group leaders will maintain configuration management of the portal content.

**12.4.5. Content Data Management.**

TJCSG sub-group leaders and document originators will review on a monthly or more frequent basis portal content to assure accuracy.

## BRAC FOUO

### 13. Computer Security.

- 13.1. **Safeguarding the Computers.** All TJCSG members will ensure that they safeguard electronic sensitive information on their computers. This includes ensuring computers are locked and incapable of use by unauthorized individuals should the owner leave the immediate work area. Microsoft software provides the capability to engage the screensaver and automatically lock the computer after a designated number of minutes. All TJCSG members should set this feature to automatically lock their computer if it is left unattended for five minutes.
- 13.2. **Transporting Data Storage Devices.** Only authorized TJCSG individuals will be allowed to transport data storage devices (e.g., laptop computer, zip/floppy disk, etc.) into or out of designated secured office spaces. This procedure may be necessary to support briefings to TJCSG principals during Pentagon meetings or move sensitive data between office locations. If exercised, this process will be strictly controlled to ensure information security and protection of data throughout. This authorized exception to policy provides necessary flexibility to the TJCSG and may be preferred over transmitting sensitive information between locations via email. Data removed will be promptly returned to the storage area when no longer needed. A list of individuals authorized to transport this data can be found at Appendix F.

### 14. Meeting Minutes and Record Keeping.

- 14.1. **TJCSG Meeting Minutes.** The TJCSG Principals will make all deliberative decisions at the TJCSG Principal meetings. Minutes for all the TJCSG Principal meetings will be signed by the Chairman of the TJCSG and maintained in an approved secure office space. The TJCSG minutes will record key points, decisions, actions, and future actions considered during the work group session, an attendance, date/time/ location of the meeting as minimum. The OSD BRAC office will be provided a copy of these minutes.
- 14.2. **CIT Meeting Minutes.** Minutes of the CIT meetings will be documented and published. The CIT chair will sign the minutes and maintained in approved secure office space. The CIT minutes will record key points, information exchanged, action item list and any future actions considered.
- 14.3. **Subgroup Meeting Minutes.** Minutes of the subgroup or team meetings are not required. Subgroups are decision recommendation bodies. If a subgroup session affects TJCSG mission, the Subgroup leader or designated representative will notify the CIT or the TJCSG for a decision need.
- 14.4. **Records Keeping.** The TJCSG administrator will develop and maintain records in a timely manner of all of the following types of information:

14.4.1. Signed Nondisclosure Agreements.

DRAFT DELIBERATIVE DOCUMENT-FOR DISCUSSION ONLY – DO NOT RELEASE UNDER FOIA

## BRAC FOUO

14.4.2. Minutes of all Principal Meetings of the TJCSG.

14.4.3. Directives

14.4.4. emails

14.4.5. All data, information, and analyses considered in making TJCSG BRAC 2005 recommendations.

14.4.6. Listing of all TJCSG members and their titles.

14.4.7. A roster containing access list for sensitive BRAC information.

**14.5. Archiving TJCSG Information.** The TJCSG information and documents will be scanned and converted into PDF format where possible and stored electronically on a CD or server temporarily while process to archive BRAC information in general is being developed by the OSD BRAC office.

### 15. 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, BRAC recommendations will be based solely on information that is certified as accurate and complete to the best of the certifier's knowledge and belief. Open source information does not need to be controlled.

### 16. Office Procedures for Correspondence.

All paper or electronic material considered deliberative in nature must be safeguarded. Correspondences and documents will contain BRAC FOUO in the header and the following information in the 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

### 17. Updating the Document.

Changes to this Information Control Plan may be required periodically throughout the BRAC 2005 process. The TJCSG members, associates, and subgroups may recommend controls and procedures updates to the CIT for interim approval, however, the TJCSG or CIT chair must approve all changes. Proposed changes will also be coordinated with the TJCSG IG representative prior to approval.

DRAFT DELIBERATIVE DOCUMENT-FOR DISCUSSION ONLY – DO NOT RELEASE UNDER FOIA

## **18. Continuity of Operations Planning (COOP)**

At times of disaster or degraded operations due to unforeseen circumstances it is crucial that alternate information storage sites, personnel, and equipment are available to provide TJCSG information and support.

If secondary, tertiary, or alternate means of operations are needed to execute the TJCSG missions, the TJCSG members, associates, and BRAC 2005 participants will recognize that the TJCSG performance, schedule and resource requirements will be degraded or changed.

### **18.1. Storage of Information**

#### **18.1.1. Primary Information Storage Site**

The primary storage site for TJCSG information (paper or electronic form) is the TJCSG Crystal City office spaces. The Analysis team will routinely provide TJCSG information to the secondary information storage site to facilitate continuity of operations.

#### **18.1.2. Secondary Information Storage Site**

The secondary storage site is the OSD BRAC office. The OSD BRAC Office staff is prepared to provide TJCSG personnel TJCSG data as mission requires.

#### **18.1.3. Tertiary Information Storage Site**

TJCSG members and associates will maintain their individual working files for a period of 180 days. These working files will be retained in order to reconstruct TJCSG document in case of primary or secondary storage site failure. Working files will be maintained in accordance with the TJCSG information control procedures.

## **19. Plan end Date.**

The execution period of this plan ends 180 days after the Secretary of Defense submits his BRAC recommendations to the BRAC Commission or as directed by the DDR&E.

## **20. Closing Remark.**

The controls implemented by this document will ensure the integrity of the information used by the TJCSG in its analysis and adheres to the guidance issued by the Secretary of Defense.

DRAFT DELIBERATIVE DOCUMENT-FOR DISCUSSION ONLY – DO NOT RELEASE UNDER FOIA

BRAC FOUO

Reviewed by:



Mr. Alan R. Shaffer

PENDING UPDATE

Chair, Capabilities Integration Team  
Technical Joint Cross Service Group

Approved by:

Dr. Ronald Sega

Chair, Technical Joint Cross Service Group

Reviewed by: Concur with Comments (TAB B )

Mr. Roger H. Florence

Audit Project Manager, Office of the Inspector General, DoD

DRAFT DELIBERATIVE DOCUMENT-FOR DISCUSSION ONLY – DO NOT RELEASE UNDER FOIA

## APPENDIX A

### Acronyms

ATL – Acquisition, Technology, and Logistics

BRAC -- Base Realignment and Closure

CIT – Capability Integration Team

COBRA- Cost of Base Realignment Actions

D&A – Development and Acquisition

DDR&E – Director, Defense Research and Engineering

DoD – Department of Defense (also referred to as the Department)

FOIA – Freedom of Information Act

FOUO – For Official Use Only

GSA- General Services Administration

ISG – Infrastructure Steering Group

OSD – Office of the Secretary of Defense

ODDRE -- Office of the Director, Defense Research and Engineering

PDA- Personnel Digit Assistant

RDATE – Research, Development, Acquisition, Test and Evaluation or RDA&TE

SIPRNET- Secret Internet Protocol Router Network

SOP- Standard Operating Procedures

TJCSG – Technical Joint Cross Service Group

USD – Under Secretary of Defense

## APPENDIX B Risk Assessment

Risk Area	Risk Area Description	Risk Mitigation
TJCSG working papers and documents	During the course of day-to-day business TJCSG members will develop working papers and correspondences memorandums and working papers. They are generally unclassified in nature; however, they may be sensitive information in nature.	The documents will contain distinctive marking and will be stored in a locked container when not in use and destroyed appropriately.
TJCSG Restricted Data/Information Approved scoring plan - Approved weights	As the process evolves the TJCSG members will develop detailed analysis plans, evaluation criteria, equations, metrics, scoring plans, alternatives, scenarios and BRAC recommendations.	Develop standards and procedures. Take steps to protect the restricted information without jeopardizing the conduct of the day-to-day business. Data will be maintained at the secure analysis facility at NC-1 unless otherwise approved by CIT chair or his/her designee.
Communication- telephones, facsimile, emails	During the course of day-to-day business the TJCSG members will use email, telephones, conference calls, and facsimile.	Establish plan and process. Take steps to improve communication among TJCSG members.
Receiving/storing BRAC Certified data - Data call responses from the services	The TJCSG will receive OSD certified official BRAC data collected from services on various data calls	Develop SOP that deals with storing and performing analysis of these official data.
Performing analysis, generating scenarios, developing alternatives and recommendations Capacity analysis MV analysis Optimization Generate scenarios - BRAC recommendations	The TJCSG will perform analysis and develop BRAC recommendations, alternatives, and document decisions on Technical facilities for ISG/OSD consideration.	Develop steps to protect BRAC sensitive information.

BRAC FOUO

**APPENDIX C**

**Security Procedures for the Technical Joint Cross Service Group  
(TJCSG)  
Office Spaces Located at Crystal City**

DRAFT DELIBERATIVE DOCUMENT-FOR DISCUSSION ONLY – DO NOT RELEASE UNDER FOIA

## BRAC FOUO

### C1.Introduction

These Standard Security Procedures (SSPs) implement security policies governing the use of the BRAC 2005 Technical Joint Cross Service Group (TJCSG) office spaces located in Crystal City. These SSPs are provided in accordance with the Security guidelines of Ref (a). The management controls that will guide and regulate the TJCSG actions to comply with the FY 2005 requirements of reference (b) (the Act), as implemented by references (c) and (d) are highlighted in the OSD Internal Control Plan (ICP) for the Base Realignment and Closure Process. This SSP complies with all provisions of the OSD ICP. All users of the TJCSG spaces are required to read and understand the contents of this SSP document. Questions about these Standard Operating Procedures should be addressed to the TJCSG Chair or the TJCSG CIT Chair.

### C2.Facility

TJCSG spaces are located at 2511 Jefferson Davis Highway in Arlington, VA. The building is in an area of Arlington referred to as Crystal City and the building is referred to as either National Center 1 (NC-1) or Presidential Towers 1 (PT-1). The TJCSG spaces are in Suite 2200. The TJCSG office spaces are approved to contain and process classified materials up to and including SECRET. Standard operating hours are Monday through Friday (0600 to 1800). At least one TJCSG authorized person will be physically in the facility whenever the TJCSG office spaces are open. The TJCSG office spaces will be used for the duration of the BRAC 2005 effort to house and store all TJCSG BRAC data. The majority of analysis and deliberative sessions will occur in these spaces. The core analytical team will predominately occupy these spaces.

### C3.Facility Access Control

Access to the TJCSG facility is controlled primarily by the certified combination lock and cipher lock on the entry door. The certified combination lock on the entrance door with a four-column digital combination is electronically modified for the TJCSG. Combination to this lock will be given to only Security Officer, Office Administrator and lead TJCSG analyst. These three people will be responsible for opening and closing the facility. The combination for secondary cipher lock on the door has been set and will be the method of entry during the working day with both locks set for after working hours. Key pad code for the cipher lock will be given to the authorized members of the Analysis Team, the TJCSG support staff, CIT members, and Subgroup Leads. Additional personnel may be designated by the TJCSG chair or CIT chair on as needed basis. Each individual receiving the key code will sign a "Key Control" form at the time the key code is provided. A listing of individuals having been granted key code access will be maintained by the TJCSG Facility Manager.

Only personnel with need-to-know and who have signed Non-Disclosure Agreements (NDA) shall have access to the facility. Personnel needing access must submit a NDA to the TJCSG administrator as well as an Access Request form, which will be reviewed and approved/disapproved by the TJCSG chair or CIT chair. In the event a person completes

DRAFT DELIBERATIVE DOCUMENT-FOR DISCUSSION ONLY – DO NOT RELEASE UNDER FOIA

## BRAC FOUO

BRAC effort and no longer requires access to the TJCSG spaces, all combinations (cipher locks, safe files, etc.) must be changed within three working days.

### C4. Media

All media entering and leaving the TJCSG office spaces must be clearly marked with the appropriate approved classification or sensitivity media label.

#### C4.1. Marking

##### C4.1.1. Classified

All classified information must be clearly marked to identify the highest classification of the material. It is the responsibility of the originator of the material to mark classified information properly. Cover sheets must be placed on the front and back of all formal classified paper materials generated to identify the highest classification level contained within. Media and Automated Information Systems (AIS) computers must be marked with the appropriate media label to identify the classification level of information contained within. Unclassified media must also have the proper label attached. Following are required markings for all classified materials, including classified media. Examples of classified marking are shown in SECNAVINST 5510.36, Chapter 6. Overall classification of material (for media, the appropriate media labels are used; this is to include unclassified media)

- Agency or facility of origin
- Date when created
- Downgrading statement
- Derived From:
- Declassify On:
- Page markings
- Portion markings
- Additional warning notices (if necessary)
- Document subject or title (generally unclassified)
- Distribution statement
- Destruction notice (if necessary)

##### C4.1.2. BRAC Sensitive

All BRAC documentation or information must be clearly marked to indicate the sensitive nature of the material. It is the responsibility of the originator of the material to mark sensitive information properly. Cover sheets must be placed on the front and back of all formal BRAC sensitive paper materials. Media and Automated Information Systems (AIS) computers must be marked with the appropriate media label to identify the classification level of information contained within. Unclassified media must also have the proper label attached.

DRAFT DELIBERATIVE DOCUMENT-FOR DISCUSSION ONLY – DO NOT RELEASE UNDER FOIA

## **C5.Computer Systems**

The TJCSG office spaces contain both unclassified and classified computer systems located throughout the facility. To identify classified and unclassified systems, media labels placed on the computer components must be easily visible by authorized users. This is to deter unclassified media from inadvertently being used to download classified information. Usage of the classified systems for SIPRNET access is strictly limited to those with SIPRNET addresses on file at the TJCSG Offices. Classified computers will be assigned on an as-needed basis and usage will be limited, as the computers will operate in shared-mode only.

The network environment for the TJCSG will be part of the Navy Marine Corps Intranet (NMCI). All users who have access to TJCSG systems are required to sign the NMCI User Agreement form. It is not anticipated that the certified BRAC data will be put on NMCI network.

The Security Officer and Facility Manager (and/or appointed alternates) must be notified when a computer used temporarily (e.g. laptop) enters the TJCSG office spaces. If computer equipment is used temporarily within the TJCSG office spaces a justification by the user to the Security officer or alternate will be submitted with the purpose.

## **C6.Storage**

### **C6.1. Classified**

GSA-approved security containers for the storage of classified materials are located in the TJCSG facility. The combinations for the classified container will be granted to limited users and will be determined by the TJCSG Security Officer. It is the responsibility of the user to ensure the Security Container Check Sheet (Form 702) is properly used when opening and closing a container. Any compromise and/or repairs must be reported to the TJCSG Security Officer. Money, personal items, etc., must not be stored in security containers.

### **C6.2. BRAC Sensitive**

GSA-approved security containers for the storage of unclassified sensitive BRAC materials are located in the TJCSG facility. Combinations to storage containers are issued by the TJCSG Security Officer. It is the responsibility of the user to ensure the Security Container Check Sheet (Form 702) is properly used when opening and closing a container. Any compromise and/or repairs must be reported to the TJCSG Security Officer. Money, personal items, etc., must not be stored in security containers.

## **C7.Destruction**

DRAFT DELIBERATIVE DOCUMENT-FOR DISCUSSION ONLY – DO NOT RELEASE UNDER FOIA

## BRAC FOUO

### **C7.1. Classified**

Classified media must be destroyed by approved destruction methods. See security Officer for process.

### **C7.2. BRAC Sensitive**

Sensitive materials may be destroyed by shredding. Media must be degaussed prior to disposal. A shredding machine is located in TJCSG spaces. This shredder will handle both paper and CD's. If a malfunction exists, or if further information is needed, contact the TJCSG Security Officer. DO NOT put sensitive BRAC printouts or sensitive BRAC media in the recycle bins. All BRAC printouts and media will be disposed of through shredding.

## **C8.Reproduction**

The copy machine in Suite 2200 is approved for the reproduction of unclassified material only. Copier machine will be placed at or within the view of the security officer. Unclassified printers are located throughout the TJCSG and are marked with media labels visible to the user. Unclassified computer systems located within the TJCSG are connected to the various printers.

## **C9.Security Violations**

For the purposes of BRAC 05, a security violation is any incident that involves the loss, compromise, or suspected compromise of classified information and or unclassified BRAC sensitive information.

### **C9.1. Improper Handling of Information**

#### **C9.1.1. Classified**

A security infraction is any incident involving improper handling of classified information in which classified information is not subject to compromise. Possible examples are classified material that is improperly or incompletely marked or improperly mailed, shipped, addressed, packaged, handled, or transmitted. All such incidents must be reported to the TJCSG Security officer.

#### **C9.1.2. BRAC Sensitive**

Improper handling or misuse of unclassified BRAC sensitive information will be reported to the TJCSG or CIT Chair and will be handled on a case-by-case basis.

DRAFT DELIBERATIVE DOCUMENT-FOR DISCUSSION ONLY – DO NOT RELEASE UNDER FOIA

### C10. Visitors

A Common access Card (CAC) is required for entry into NC-1. If the visitor does not possess a CAC badge, two forms of picture identification will be required prior to entry into the building, assuming a visitor clearance is on the file. For the purpose of entry into the TJCSG office spaces, Visitors are considered to be those individuals who have not signed the BRAC non disclosure form, do not have a need-to-know, and are not on the access control list. This includes janitorial, maintenance, and delivery personnel not assigned to the TJCSG, and not working on BRAC-related issues. All visitors must contact the TJCSG facility coordinator and sign the visitor log prior to entering the TJCSG office spaces. All visitors will be escorted, and it is the responsibility of the host to maintain visual contact. Note that a visitor may have a security clearance, but not necessarily the need-to-know.

### C11. Communication Security (COMSEC)

Individuals accessing COMSEC materials must have the proper clearance level and need-to-know, and have a signed CMS Responsibility Acknowledgment Form. TJCSG currently has an area approved to store and operate COMSEC material. An access list-identifying individual authorized to handle COMSEC material is located in the Facility manager's office.

### C12. Emergency Procedures

These emergency procedures define the course(s) of action in the event of any type of emergency having a general effect upon classified and/or BRAC sensitive materials or personnel. A copy of this emergency procedure is posted near the entrance door in room C327 and contained within this TJCSG SSP.

Safety must always take precedence over security issues regarding classified or sensitive BRAC material. The TJCSG Management and the TJCSG Security Officer must be notified immediately when an emergency occurs.

Those listed below, or the senior individuals with access who are present in the facility during an emergency, are authorized to implement these procedures.

COL Peter DeSalva  
Work Phone: 703-432-3444  
Home Phone: 703-377-5545

COL Robert Buckstad  
Work Phone: 703-695-0552  
Home Phone: 703-375-9487

Ms. Eileen Shibley  
Work Phone: 703-602-6424  
Home Phone: 703-382-8975

CDR Dave Faulk  
Work Phone: 703-602-6416  
Home Phone: 703-542-5205

## BRAC FOUO

Dr. Jim Short  
Work Phone: 703-696-2529  
Home Phone: 703-375-1348

Mr. Gary Strack  
Work Phone: 703-614-7012  
Home Phone: 703-446-6051

Any of the above listed individuals may direct emergency procedures. It is the responsibility of all assigned personnel to assist these individuals.

### **C12.1. Actual Fire or Explosion**

In the event of a fire or explosion, dial 911 and immediately pull the handle to the alarm box located on the west wall near the entrance door of Suite 3500. Several fire extinguishers are located throughout the TJCSG spaces and may be used to contain the fire until the Arlington Fire Department arrives. When reporting an emergency, be sure to tell the dispatcher (1) the type of incident, fire, or explosion; and (2) the specific location. You should also:

Notify other personnel in the area.

Meet and guide emergency personnel to the area.

Remain in the immediate vicinity to facilitate the admission of the firemen. Do not impede the firemen in any way in the performance of their duties.

Notify one of the personnel listed above.

If a fire, explosion, or other serious incident occurs within the facility during non-working hours, the responding individual shall notify emergency personnel (if not already at the facility) and the personnel listed above.

### **C12.2. Threat of Fire or Explosion**

If a fire, explosion, or other serious incident in the area adjacent to the facility threatens the security of TJCSG classified or BRAC sensitive material, and if time and the situation allow, all classified and BRAC sensitive material should be secured in containers designated for its protection.

## BRAC FOUO

### References:

- a. SECNAVINST 5510.3 Defense Base Closure and Realignment Act of 1990 (Sections 2901 – 2914 of P. L. 101 – 510, as amended)
- b. SECDEF memo of 15 nov 02; Subj: Transformation Through Base Realignment and Closure USD (AT&L memo of 16 Apr 03; Subj: Transformation Through Base Realignment and Closure (BRAC 2005) Policy Memorandum One – Policy, Responsibilities, and Procedures
- c. DoD 5200.1R

DRAFT DELIBERATIVE DOCUMENT-FOR DISCUSSION ONLY – DO NOT RELEASE UNDER FOIA

BRAC FOUO

Appendix E: CLOSE HOLD Cover Page

DRAFT DELIBERATIVE DOCUMENT-FOR DISCUSSION ONLY - DO NOT RELEASE UNDER FOIA

---

# CLOSE HOLD

---

Material contained herein is sensitive. Release of data or analysis pertaining to evaluation of military bases for closure or realignment is restricted until the Secretary of Defense forwards recommendations to the Defense Base Closure and Realignment Commission in May 2005. All individuals handling this information should take steps to protect the material herein from disclosure.

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



**Director, Defense Research & Engineering**

**Room 3E1014  
(703) 697-5776**

# CLOSE HOLD

## BRAC FOUO

### **Appendix F: List of Authorized Individuals to Transport Sensitive BRAC DATA**

(In process)

The CIT Chair and CIT Executive shall maintain the official list of authorized personnel to transport sensitive BRAC data. Only the CIT Chair and Executive are authorized to grant additional authorized couriers. When the list is finalized, the TJCSG staff security oversight manager shall update the Appendix F.

Coordination Pages **Tab B**

Coordination Page for:

SUBJECT: Transformation through Base Realignment and Closure Technical Joint Cross Service Group (TJCSG) Information Control Procedures (ICP)

Mr. Roger Florence, DOD IG	Concur with Comments
Dr. Bob Rohde, Army CIT Representative	Concur with Comments
Mr. George Ryan, Navy CIT Representative	
Mr. Al Goldstyan, Air Force CIT Representative	
Mr. Matt Mleziva, C4ISR Subgroup Spokesperson	Concur
Dr. Larry Schuette, Innovative Systems Subgroup Spokesperson	Concur
Dr. Karen Higgins, Weapons & Armaments Subgroup Spokesperson	Concur
Mr. Thom Mathes, ALSS Subgroup Spokesperson	Concur
Dr. William Berry, Enabling Technology Subgroup Spokesperson	Concur
COL Pete DeSalva, Analytics Group Spokesperson	Concur