Intelligence Joint Cross-Service Group Standard Operating Procedures (SOP) As of January 2004

PURPOSE

This plan establishes the policies and responsibilities that constitute the Intelligence Joint Cross-Service Group (IJCSG). It is to be used to implement the Defense Base Closure and Realignment (BRAC) Act of 1990 (P.L. 101-510 as amended); the Secretary's November 15, 2002, "Transformation Through Base Realignment and Closure" "Transformation Through Base Realignment and Closure (BRAC 2005) Policy Memorandum One – Policy, Responsibilities, and Procedures;" the OSD BRAC Internal Control Plan (ICP); and all subsequent policy memoranda outlining the DoD BRAC 2005 process.

INTERNAL CONTROL MECHANISMS

The following outlines controls for the IJCSG to ensure all BRAC 2005 information used to develop and make realignment and closure recommendations submitted to the Secretary of Defense and/or the 2005 Defense BRAC Commission must be certified, as accurate and complete to the best of the certifier's knowledge and belief, and auditable. The Military Departments and Defense Agencies will establish similar document controls for the Defense intelligence related BRAC processes.

The BRAC process will be recorded and clearly documented to ensure the integrity of the process performed by the IJCSG. Furthermore, controls will be implemented to ensure that the information used by the IJCSG in its analysis is certified accurate and complete, and that the information is used consistently by OSD, the Military Departments, and the Defense Agencies throughout the BRAC 2005 process. To protect the integrity of the BRAC 2005 documentation prepared, handled, or processed, the IJCSG will adhere to the following control elements:

> Data Collection: Information used for analyses and/or decision-making will be obtained from the Military Departments and Defense Agencies. The mechanism for requesting IJCSG data from the

Military Departments and the Defense Agencies will be in the form of electronic and/or hard copy information requests issued to the Military Departments and Defense Agencies. The Military Departments and Defense Agencies will use their Service BRAC processes, in coordination with their Service intelligence chiefs, and directors, respectively for collecting the requested information and ensuring such information is certified accurate and complete before it is forwarded to the IJCSG. Only certified information will be used to develop BRAC 2005 recommendations. Each Military Department and Defense Agency will coordinate their responses, as required, with all appropriate organizations, to include the Joint Chiefs of Staff, J2 and the Combatant Commands.

Classified Data: Every effort will be made by the Military Departments and Defense Agencies to provide complete responses at the lowest level of classification possible. The Military Departments and Defense Agencies will classify every data element it provides to the IJCSG. All classified responses to data calls and requests for information will be provided using DoD approved secure means.

All IJCSG members will possess at a minimum a TS/SI/TK/B/G/HCS security clearance. Only IJCSG Principal, Alternate, or Observer members will attend deliberative IJCSG discussions. Representatives for either the Principal or Alternate will not be permitted. All IJCSG meetings will be held in an appropriately certified SCIF (location to be determined).

The IJCSG will collect, aggregate, analyze, and store data for the BRAC 2005 process up to the TS/SI/TK/B/G/HCS level, as necessary, in an appropriately approved, compartmented, standalone computer that is restricted to a few, fully cleared, personnel with a documented "need to know." This computer will be housed in an appropriately approved DoD Sensitive Compartmented Information Facility (SCIF). If and when it proves necessary, the Chair, IJCSG will ensure special security measures are implemented to accommodate special access program information. The Chair, IJCSG will work with each Defense intelligence community component to ensure all classified data is fully protected in accordance with relevant security policies and regulations.

All classified information produced by the IJCSG will be handled and stored in accordance with DoD regulations for classified material. All substantive and deliberative information will be centrally stored at the IJCSG's SCIF. Access to such information will require appropriate security clearances, a clearly demonstrated "need to know," and the IJCSG Chair's prior permission. The IJCSG will maintain an access list for their respective centrally stored documents. The access list will indicate the name of the individual who was provided access to the stored material, the individual's organization, the specific documents that were reviewed, and the date the information was reviewed.

The standard OSD BRAC 2005 CLOSE HOLD cover sheet will protect all hardcopy unclassified documentation. Unclassified deliberative documents will be treated as CONFIDENTIAL. The appropriate DoD approved cover sheet for classified information will be used for actual classified data. All IJCSG and subordinate working group members will adhere to the IJCSG's SOP. The Chair, IJCSG and subordinate working group chairs will be responsible for establishing and maintaining an effective document control program. Copies of classified documents will be numbered and provided to the IJCSG members and working group participants only. Additional copies of such documents are prohibited without the prior permission of the Chair, IJCSG. Electronic forwarding of such documents also is prohibited without the permission of the Chair, IJCSG. If electronic or hardcopy copies are produced, the Chair, IJCSG must be told who the additional recipients are and how many copies were provided. A master controlled documents registry will be maintained that indicates the total number of approved copies and the number of copies per approved custodian.

Certification: Any data file forwarded to the IJCSG by the Military Departments or Defense Agencies must be certified by the Service BRAC process, in coordination with the Service intelligence chief and director, respectively, and transmitted through secure channels. Data and information gathered from authoritative or official sources external to DoD need only be certified as to the source if the sources'

accuracy can be determined by the audit community in accordance with U.S. General Accounting Office (GAO) guidance.

Record Keeping: Minutes will be maintained of all IJCSG meetings. Minutes are not required for IJCSG subgroup meetings. Unless the classification of the minutes prohibits it, the OSD BRAC office also will retain a copy. The IJCSG will record attendance, provide a synopsis of items discussed and include all decisions and recommendations. The Chair, IJCSG will be responsible for overseeing and enforcing attendance at each meeting as well as approving substitutions on a case-by-case basis. The Chair, IJCSG will also be responsible for ensuring that only certified data provided by the Military Departments and Defense Agencies is used in the deliberative process. The overall responsibility for safeguarding BRAC 2005 data and information rests with the Chair, IJCSG. However, this does not relieve each and every individual involved in the BRAC 2005 process from the responsibility to protect internal/deliberative information involved in the BRAC 2005 process.

Oral Briefings: On occasion, the IJCSG may receive formal and informal briefings from inside and outside the Federal Government. To ensure a record of all information provided to these groups is maintained, the content of all oral briefings will be captured in the minutes prepared for the meetings at which a particular briefing was presented. All briefing slides and electronic presentations will be attached to the minutes recorded for the meeting. While these briefings may be useful in developing policies or suggesting methods for making measurements or evaluations, no data from such briefings will be accepted by the IJCSG, unless such data is independently validated and certified in accordance with these procedures.

Outside Studies: During the BRAC 2005 process, studies and reports that originated outside the process may be brought to the attention of any designated BRAC group. While these studies may be useful in developing policies and/or suggesting methods for making measurements or evaluations, no data from such briefings may be accepted by the IJCSG, unless such data is independently validated and certified in accordance with the BRAC 2005 procedures.

Technical Experts: Technical experts may be used to support the development and/or the refinement of the analytical efforts of the IJCSG. The Military Departments and Defense Agencies will identify such technical experts to the IJCSG and each individual will be briefed on the sensitivity of BRAC data. The IJCSG will maintain a list of individuals authorized to access their data. When technical experts provide information, expertise, or data that the IJCSG considers relevant and appropriate for analyses, the experts shall be requested to submit the information or data in writing with the required certification. Technical experts will be granted limited access to BRAC 2005 data and information that will allow them to assist the IJCSG in the development and/or refinement of analytical efforts. The use of technical experts will be communicated, either orally or in writing, to the ISG.

Non-Disclosure Agreements: Each IJCSG member will sign a BRAC 2005 non-disclosure agreement. Additionally, all other individuals working within the process or providing support to the process (including IG DoD, technical experts, contractors, etc.) will be required to sign non-disclosure agreements. (The DoD standard agreement is at Appendix C to "Transformation Through Base Realignment and Closure (BRAC 2005) Policy Memorandum One – Policy, Responsibilities, and Procedures" memorandum). However, signing a Non-Disclosure Agreement does not grant access to BRAC data beyond a need-to-know basis.

ACCESS to BRAC 2005 INFORMATION

To protect the integrity of the BRAC 2005 process, all files, data, and materials relating to the 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 and the USD(I) with respect to the IJCSG. All BRAC 2005 documents, including electronic media, will have the following statements as header and footer, as appropriate:

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 members of the IJCSG are entrusted to have access to the BRAC 2005 data and information that originated from either the Military Departments or the Defense Agencies. Consistent with the organization controls set forth in this ICP, access will not be granted to any individual, to include technical experts or outside consultants, without the consent of the Chair, IJCSG. Such access carries a responsibility for ensuring that BRAC 2005 data and information is treated as sensitive and pre-decisional. The members of the IJCSG are required to protect the BRAC 2005 process from either improper or unofficial disclosures. The Chair, IJCSG will ensure all assigned and substitute members of the group are informed that no internal deliberations or data will be discussed or shared with anyone outside the group without specific Chair approval. The group members must also take precautions to prevent the acceptance of information that is not certified or may be forwarded to the IJCSG through channels other than those identified in this document and BRAC 2005 policy guidance.

Coordination with the DCI: Including Defense intelligence in the BRAC 2005 process will impact the entire U.S. Intelligence Community. Therefore, it is imperative that the IJCSG coordinates fully with the Director, Central Intelligence (DCI) on its activities and recommendations. A DCI designated staff representative will be invited to attend IJCSG meetings as an observer. The IJCSG will provide periodic updates to the DCI and the USD(I) as appropriate. The USD(I) will serve as the focal point for IJCSG coordination with the DCI on security matters that cannot otherwise by resolved.

Sensitive TOP SECRET CODEWORD level information will be made available upon request within the IJCSG SCIF to the following individuals on a need to know basis after the Secretary's recommendations are released on 15 May 2005:

- Chair and Ranking Member of the SASC and HASC
- Chair and Ranking Member of the HPSCI and SSCI
- Majority and Minority Leaders of the House and Senate
- Appropriately cleared members of the BRAC Commission
- Select others – approved by the USD(I) on a case-by-case basis.

AUDIT ACCESS TO RECORDS

The Comptroller General is required to submit a report to Congress and the Commission containing a detailed analysis of the Secretary's recommendations and selection process shortly after the Secretary provides his BRAC recommendations to the Commission. To facilitate this review, the Department will allow appropriately cleared GAO auditors full and open access to all elements of the DoD process, except for deliberative meetings, and to all data supporting the Secretary's final recommendations, as it is being developed and implemented. Copies of the deliberative meeting minutes will be made available to the GAO after the Chair signs them.

Full and open access to the BRAC 2005 process and data will be granted to appropriately cleared personnel of the Inspector General of the Department of Defense. Furthermore, appropriately cleared personnel of the audit agencies of the Military Departments and Defense Agencies participating in BRAC 2005 will review and validate data collected and analyzed by their Departments and Agencies. GAO, the DoD Inspector General, and the relevant audit agencies will coordinate their efforts to avoid duplication of effort.

DISSEMINATION

All members of the IJCSG must use every precaution to prevent the improper release of and/or access to the BRAC 2005 data and 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 through telephone conversation, facsimile "FAX," or electronic "E-mail" transmission. Secure FAX machines and E-mail systems will be used to transmit not only classified information, but also unclassified, but sensitive IJCSG information. Classified information will be provided only to personnel with the appropriate security clearance and a documented need to know. Secure dissemination channels will be used for

all classified information. Dissemination of information that is not discussed in the SOP will only be made with the expressed documented approval of the USD(AT&L) and the USD(I). The USD(AT&L) and USD(I) will be advised of any control violations or weaknesses that are identified through application of this SOP or of any modifications that may be needed.

CHANGES TO SOP

As the USD(AT&L) and USD(I) issues supplemental guidance that affects this SOP, the IJCSG will incorporate this guidance into this SOP. Additions/deletions/revisions to this list of procedures requires the permission of the Chair, IJCSG.

Carol A. Haave
DUSD(I) CI&S
Chair, IJCSG

INTELLIGENCE JOINT CROSS SERVICE GROUP (IJCSG)

SECURITY STANDARD OPERATING PROCEDURES

July 2004

IJCSG Security Manager
Lyn Young

Approved By

Carol A. Haave
Deputy Under Secretary of Defense
(Counterintelligence and Security)
Chair, Intelligence Joint Cross-Service Group (IJCSG)

FORWARD

The Intelligence Joint Cross Service Group (IJCSG) as part of the Base Realignment and Closure (BRAC) process is evaluating intelligence equities that support both the Department of Defense and the Intelligence Community. At the 21 November 2003, Infrastructure Steering Group (ISG) meeting, serious concerns were raised regarding the unprecedented inclusion of highly classified Intelligence information in the BRAC process.

However, upon review, the DoD OGC and DCI Community Management Staff Chief Legal Counsel have since determined that the BRAC statutes are not inconsistent with the Departments' legal responsibilities for protecting classified information. Further, there is ample precedent for handling highly sensitive information in support of commissions and Congress. Based upon these precedents and a review of applicable security directives, the attached Standard Operating Procedures (SOP) has been developed.

This SOP is applicable to the Intelligence Joint Cross-Service Group's (IJCSG), Sensitive Compartment Information Facility (SCIF) and establishes areas of security management responsibility for the protection of highly classified material. Each person authorized access to this SCIF shall certify in writing they have read and understand contents of the SOP and shall follow the procedures outlined therein.

The document is drawn from the DoD policies and directives governing security procedures within the Defense Intelligence Community. The SOP builds upon the existing Defense Intelligence Agency certified Technology Integration Center SOP (Attachment A) and Standard Practices and Procedures (Attachment B), developed for the multi-level secure facility in which the IJCSG Core Team is a tenant. This facility is the Defense Advanced Research Projects Agency (DARPA) Technical Integration Center. Therefore, this SOP not only works in tandem with the aforementioned documents; it cannot be viewed apart from those documents. Additionally, a Co-utilization agreement has been signed between DARPA and the IJCSG.

Security is everyone's responsibility and the protection of the very sensitive data is paramount. The Point of Contact for issues regarding this SOP is the IJCSG Security Manager, Lyn Young at (703) 769-9450.

Carol A. Haave
Deputy Under Secretary of Defense
(Counterintelligence and Security)
Chair, Intelligence Joint Cross-Service Group (IJCSG)

Attachments:
As Stated

DISCLOSURE OF CLASSIFIED INFORMATION

"Whomsoever knowingly and willingly communicates, furnishes, transmits, or otherwise makes available to an unauthorized person or publishes or uses in any manner, prejudicial to the safety of interests of the Unites States or for the benefit of a foreign government to the detriment of the United States any classified information (1) concerning the nature, preparation, or use of code, cipher cryptographic system of the Unites States or any foreign government; or (2) concerning the design, construction, use, maintenance or repair of any device, apparatus, or appliance used or prepared, or planned for use by the United States or any foreign government for cryptographic or communications intelligence purpose; or (3) concerning the communication intelligence activities of the United States or any foreign government; (4) obtaining by process of communication intelligence from the communications of any foreign government, knowing the same to have been obtained by such process, shall be fined not more than $10,000 or imprisoned not more than 10 years or both."

Purposely left blank

TABLE OF CONTENTS

FOREWORD 1
TABLE OF CONTENTS 3
1.0 SOP PURPOSE AND SCOPE 8
1.1 Authority 8
1.2 Applicability 8
2.0 REFERENCE DOCUMENTATION 8
3.0 RESPONSIBILITIES 10
3.1 Security Structure for the TIC In Which the IJCSG is a Tenant 10
3.2 Security Structure for the IJCSG SCIF 10
3.2.1 IJCSG Security Manager 10
3.2.2 SCI Indoctrinated Personnel 11
4.0 INTERNAL CONTROL MECHANISMS 12
4.1 Data Collection 12
4.1.1 Classification of Data 12
4.1.1.a Classification at Lowest Level 12
4.1.1.b Classification IAW Original Source Material 13
4.1.1.c Secure Data Storage and Handling Procedures 13
4.2 Document Control 14
4.2.1 Document Control Procedures 14
4.2.1.a Data Storage 14
4.2.1.b Master Document Registry 14
4.2.1.c Document Access List 14
4.2.1.d Access to Document for People Not on Access List 14
4.2.1.e Numbered Copies of Documents 14
4.2.1.f OSD Cover Sheet 14
4.2.2 Labeling IJCSG Core Team Documents and Media 14
4.3 Certification of Data 15
4.3.1 Data Forwarded by the MilDeps or Defense Intel Agencies 15
4.3.2 Data and Information Gathered External to DoD 15
4.4 Record Keeping 15
4.4.1 Minutes of Meetings 15
4.4.1.a Master Copy of Meetings 15
4.4.1.b OSD Copy of Minutes 16
4.4.1.c Numbered Copy of Minutes for IJCSG Core Team 16
4.4.1.d Minutes of IJCSG Core Team Meetings 16
4.4.2 Record of Clearances 16
4.4.3 Nondisclosure Agreements 16
4.4.3.a Personnel Responsible for Signing NDA 16
4.4.3.b Responsibility for Maintaining File of NDAs 16
4.4.4 Approved BRAC Documents 16
4.4.5 Core Team Non-Deliberative Notes and Working Papers 16
4.4.6 Information Provided by Technical Experts 17
4.4.6.a Procedures for Technical; Experts 17
4.4.6.b Certification of Information Provided by Technical Experts 17

4.5 Access to BRAC Information 17
4.5.1 IJCSG Members Access to BRAC Materials 17
4.5.2 Senior and Principals Access to BRAC Information 17
4.5.3 Director CIA/CMS Access to BRAC Information 17
4.5.4 Other Approved Recipients Access to BRAC Information 18
4.5.5 General Accounting Office/DoD IG Audit Access to Records 18
4.5.5.a Access to Records 18
4.5.5.b Copying Records 18
4.5.5.c IJCSG Core Team Audit Responsibilities 18
4.5.6 Miscellaneous Personnel Requiring Access to the IJCSG SCIF 18
4.6 Dissemination of BRAC 2005 Data 18
5.0 PERSONNEL SECURITY 19
5.1 Security Clearances 19
5.2 Personnel Approved for Access to the IJCSG SCIF 19
5.3 Visitors to the IJCSG SCIF 19
5.3.1 Escorting of Visitors to the IJCSG SCIF 19
5.3.1.a Categories of Visitors 19
5.3.1.b Badges 19
5.3.1.c Record Keeping 20
5.3.1.d Sanitization of the IJCSG SCIF 20
5.3.1.e Other Associated Escort Procedures 20
5.4 Incidents that Require the Notification of the IJCSG Security Manager 20
5.4.1 Administrative Incidents Requiring Notification 20
5.4.2 Incident Notification 21
5.5 Security Education 21
5.5.1 Initial Briefing 21
5.5.2 Continuing Security Education Program 21
6.0 CLASSIFIED INFORMATION SECURITY 22
6.1 Responsibility 22
6.2 Procedures for Marking Classified Documents 22
6.2.1 Overall Security Classification and SCI Notations 22
6.2.2 SCI Control System Caveats 22
6.2.3 Classification Authority 22
6.3 Transporting Classified Material 22
6.3.1 Courier Procedures 23
6.3.1.a Courier Pouch 23
6.3.1.b Wrapping Classified Material 23
6.4 Reproduction of Classified Material 23
6.4.1 Reproduction in the IJCSG SCIF 23
6.4.2 Reproduction of SCI Documents 24
6.5 Accountability for Data Call Information 24
6.6 STU III and STE 24
6.6.1 Crypton Ignition Keys and KOV-14 Cards 24
6.6.2 Procedures for STU III and STE 24
6.6.2.a Making or Receiving a Secure Call on the STU III 25
6.6.2.b Making or Receiving a Secure Call on the STE 25

6.7 TIC Secure FAX 25
6.7.1 Accreditation, Clearances and Documentation for the Secure FAX 25
6.7.1.a Accreditation for Sending and Receiving SCI Materials 25
6.7.1.b Required Clearance and Need to Know 25
6.7.1.c Control Numbers and FAX Cover Sheet 26
6.7.1.d Labels and Accountability 26
6.7.2 Transmitting a Secure FAX 26
6.7.3 Receiving a Secure FAX 26
6.8 UNCLAS Telephone 26
6.9 Equipment and Media 26
6.9.1 Accountability for Classified Equipment and Media 26
6.9.2 Movement of Classified Equipment and Media 27
6.10 Classified Working Papers 27
6.11 Personally-Owned Electronic Equipment 27
6.11.1 Electronic Equipment Permitted in the IJCSG SCIF 27
6.11.2 Electronic Equipment Prohibited in the IJCSG SCIF 27
7.0 DESTRUCTION OF DOCUMENTS AND MEDIA 27
8.0 PHYSICAL SECURITY 28
8.1 Facility Accreditation 28
8.1.1 IJCSG SCIF Accreditation 28
8.1.2 TIC Facility Accreditation 28
8.2 TIC Security Provisions 28
8.2.1 TIC Security Personnel 28
8.2.2 TIC Closed-Circuit TV 28
8.2.3 TIC Panic Button 28
8.2.4 TIC Alarm System 28
8.2.5 TIC Corridor Partitions 29
8.3 Hours of Operation 29
8.3.1 TIC Duty Hours 29
8.3.1.a Normal Duty Hours 29
8.3.1.b After-Hours 29
8.4 Opening and Closing Procedures for Room 116 29
8.4.1 Opening Procedures for Room 116 29
8.4.2 Closing Procedures for Room 116 30
8.5 Procedures for Room 117 and Room 117A 31
8.5.1 People With Access to Room 117 and 117A 31
8.5.1.a Door Combinations 31
8.5.1.b Safe Combinations 31
8.5.1.c SUN Computer Access 31
8.5.2 Opening Procedures for Room 117 31
8.5.3 Closing Procedures for Room 117 31
8.6 Emergency Evacuation Plan and Rallying Point 32
8.6.1 Evacuation Procedures 32
8.6.2 Rallying Point 32
8.6.3 Accountability 32
8.6.4 Security Containers 33

8.7 Power Loss Procedures 33
9.0 INFORMATION SYSTEMS SECURITY 33
9.1 Responsibilities 33
9.1.1 IJCSG Security Manager Responsibilities 33
9.1.2 ISSM Responsibilities 34
9.1.3 System User Responsibilities 34
9.2 Custom Applications Software 34
9.2.1 Accreditation of Custom Software 34
9.2.2 OSD Responsibilities 34
9.2.2.a Staff Support 35
9.2.2.b Funding Support 35
9.2.2.c Operator Support 35
9.2.2.d Security Support 35
9.2.3 SUN/Oracle Definitions 35
9.2.3.a Oracle Team 35
9.2.3.b Master Data Base 35
9.2.3.c Core Team Laptop 35
9.2.3.d Oracle Team Work Station 35
9.2.3.e Oracle LAN 35
9.2.3.f Oracle Parser 35
9.2.3.g Core Team 35
9.3 Data Base Transfer Procedures 35
9.3.1 Movement of Data to Master Data Base 35
9.3.2 Movement of Data from Room 117 to Room 116 36
9.4 Office Automation Systems TBD 36
9.5 Capacity Analysis Tool/Spreadsheet Template TBD 36
9.6 Military Value Scoring Plan Spreadsheet Template TBD 36
9.7 COBRA Tool TBD 36
10.0 DATA CALL DELIVERY PROCESS 36
10.1 Organizations Making Delivery 36
10.2 Procedures for Receiving Data 37
10.2.1 Data Check-in Process 37
10.2.2 Two Person Rule for Accepting Data 37
10.2.3 Document Transmittal Sheet 37
10.2.4 Storage of Data 37
11.0 DATA RETENTION, STORAGE, SEARCH/RETRIEVAL, DESTRUCTION 37
11.1 Approval Procedure 37
11.2 Data Retention 37
11.3 Procedural Changes 37

APPENDICIES

A. After Duty Recall Roster for Room 116 38
B-1. After Duty Recall Roster for Room 117 39
B-2. After Duty Recall Roster for Room 117A 40

C. SCI Control System Identification and/or Markings 41
D. Acronyms and Abbreviations 42
E. Emergency Instructions for any Emergency 44
F. IJCSG Core Team Form 45
Nondisclosure Agreement
TIC Master System Security Plan (MSSP) Education Checklist
Activity Security Checklist (SF) 701
Security Container Check Sheet (SF 702)
Facility Security Check Log
DA Form 3964 (Classified Document Accountability Record)
IJCSG Fax Cover Sheet

1.0 PURPOSE AND SCOPE

This Standard Operating Procedures (SOP) establishes the security policies and responsibilities for the IJCSG and the IJCSG Core Team working group. It will be used throughout the 2005 Base Realignment and Closure (BRAC) process. Additionally, the SOP addresses policies and procedures regarding the secure facility in which the IJCSG Core Team working group is a tenant.

The Chair, IJCSG, shall incorporate any further supplemental guidance, from the Chair, Infrastructure Steering Group, into this SOP. Any other future revisions to this SOP require the authorization of the Chair, IJCSG.

The Technology Integration Center (TIC) facility is the focal point for the activities of the IJCSG Core Team working Group. The TIC; staffed and managed by Maden Technologies, Inc., 2110 Washington Boulevard, Suite 100, Arlington, VA 22204; is a multi-level secure facility. The Defense Intelligence Agency (DIA) is the Cognizant Security Authority (CSA) for SCI at the TIC. The Defense Security Service (DSS) is the CSA for Collateral Information.

1.1 Authority

This SOP serves as both the basic statement of IJCSG policy and a guide to the implementation and enforcement of the security management program. The procedures contained in the SOP adhere to published guidance and accepted practices within the Defense Intelligence Community.

1.2 Applicability

This SOP is applicable to the IJCSG SCIF and all assigned personnel and visitors to the IJCSG SCIF. All members of the IJCSG assigned and or/authorized access to this facility are responsible for complying with and certifying in writing they understand these procedures. All changes to this SOP will be effective upon the date of receipt or as otherwise specifically indicated.

2.0 REFERENCE DOCUMENTATION

Publications applicable to the day-to-day operational requirements of the IJCSG are listed below:

- DoD 5200.1R, *Information Security Program* (U)
- DoD 8500.1, *Security Requirements for Automated Information Systems* (U)
- DoD 5220.22-M, *National Industrial Security Program Operating Manual (NISPOM)* and DoD 5220.22-M-SUP 1 (U)

- DoD 5220.22-S, *COMSEC Supplement to the NISPOM* (U)
- DoD Directive S-5105.21-M-1, *Sensitive Compartmented Information Administrative Security Manual* (U)
- DoD Directive TS-5105.21-M-2, *Sensitive Compartmented Information (SCI) Security Manual - Communications Intelligence (COMINT) Policy* (U)
- DoD Directive TS-5105.21-M-3, *Sensitive Compartmented Information (SCI) Security Manual - TK Policy* (U)
- DCID 1/16, *Security Policy for Uniform Protection of Intelligence Processed in Automated Information Systems and Networks* (U)
- DCID 1/21, *Physical Security Standards For Sensitive Compartmented Information Facilities* (U)
- DCID 6/3, *Protecting Sensitive Compartmented Information Within Information Systems* (U)
- DCID 6/4, *Personnel Security Standards and Procedures Governing Eligibility for Access to Sensitive Compartmented Information (SCI)* (U)
- DCID 6/6, *Security Controls on the Dissemination of Intelligence Information* (U)
- DCID 6/9, *Physical Security Standards for Sensitive Compartmented Information Facilities (SCIF)* (U)
- DIAM 04, *Joint DoDIIS/Cryptologic SCI Information Systems Security Standards*
- DIAM 50-5, *Sensitive Compartmented Information (SCI) Contractor Administrative Security, Vol 1* (U)
- Executive Order 12333, *United States Intelligence Activities* (U)
- Executive Order 12958, *Classified National Security Information* (U)
- TIC, *April 2003 Standard Practices and Procedures* (U)
- TIC, *April 2003 Standard Operating Procedures* (U)
- TIC, *September 2003 Master System Security Plan (SSP)* (U)
- OSD Internal *Control Plan for the 2005 Base Realignment and Closure Process* (U)

- Intelligence Joint Cross-Service Group (IJCSG), *Standing Operating Procedures* (U)

3.0 RESPONSIBILITIES

3.1 Security Structure for the TIC in which the IJCSG Core Team is a Tenant

The Macro Security Structure for the TIC facility discussed in paragraph 3.2 of the TIC Standard Practices and Procedures.

3.2 Security Structure for the IJCSG SCIF

3.2.1 IJCSG Security Manager

The IJCSG Security Manager is responsible for all security issues that take place within or pertain to the IJCSG SCIF. The IJCSG Security Manager reports to the Chair, IJCSG through the Facilitator IJCSG Core Team working group, who is ultimately responsible for all security matters.

The IJCSG Security Manager is responsible for the day-to-day management, implementation and enforcement of SCI security and administrative instructions for the SCIF. The Security Manager will:

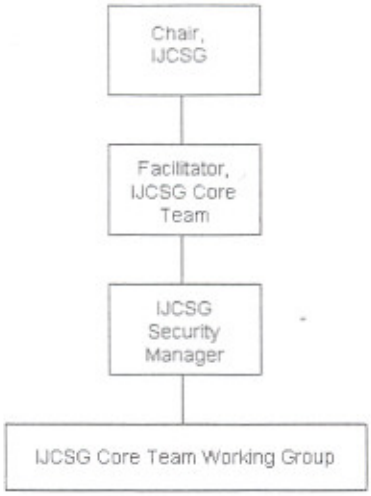
- Supervise and direct the security measures necessary to protect and safeguard classified information.
- Develop and maintain a written SOP that implements each operable security requirement.
- Develop and maintain an Emergency Action Plan for safeguarding classified information during emergencies
- Be responsible for managing and implementing the day-to-day SCI security function within the SCIF to include Personnel, Physical, Automated Information Systems, TEMPEST, Communications Security, Information Security and Operational Security.
- Ensure all SCI-indoctrinated individuals, assigned to the SCIF, are kept apprised of the requirements and guidelines for protecting SCI.
- Maintain a self-inspection program and conduct an annual evaluation of all security procedures applicable to both SCIF and office operations.
- Maintain internal procedures to ensure that all individuals are aware of their responsibilities to report any loss, compromise or suspected compromise of classified information, as well as any security violation involving classified information.

- The IJCSG Security Manager will review and update this SOP on a continuing basis.
- Ensure all assigned personnel review the SOP annually.
- Ensure all newly assigned SCI-indoctrinated personnel review and sign a sheet indicating date the document was read.
- The Security Manager is responsible for other appropriate duties as described herein.
- Maintain a list of all security clearances for personnel assigned to the SCIF.
- Verify the security clearances for all personnel entering the SCIF.
- Coordinate the passing of clearances when required.

3.2.2 SCI-Indoctrinated Personnel

All SCI-indoctrinated personnel assigned to the IJCSJ and IJCSG Core Team working group are responsible for maintaining the security of all classified information by adhering to all applicable published polices and directives. Accordingly, these personnel shall:

- Review the SOP annually; comply with its procedures, exercise individual responsibilities, and follow all other written or oral security instructions from the IJCSG Security Manager.
- Take appropriate steps to ensure classified information is not exposed when uncleared visitors are announced in the area.
- Safeguard the information related to BRAC 2005 utilizing FOUO information-handling guidelines.
- Take appropriate steps to ensure the people with whom they discuss BRAC information are appropriately cleared, have a need-to-know, and have signed a non-disclosure agreement.



IJCSG SCIF Organization Chart

4.0 INTERNAL CONTROL MECHANISMS

4.1 Data Collection

Information used for analysis and decision-making will be obtained from the Military Departments and Defense Intelligence Agencies. The IJCSG will issue the appropriate information requests in either an electronic or hard-copy format. The Military Departments and Defense Intelligence Agencies will, in turn, use their Service or Agency BRAC processes for collecting the requested information. Additionally, they will ensure the information is certified accurate and complete before it is delivered to the IJCSG. (Each Military Department and Defense Intelligence Agency will coordinate their responses, with all appropriate organizations, to include the Joint Chiefs of Staff, J2 and the Combatant Commands, as required.) Only certified information will be used to develop BRAC 2005 recommendations.

4.1.1 Classification of Data

4.1.1.a Data to be Provided at the Lowest Level of Classification Possible. Every effort will be made by the Military Departments and Defense Intelligence Agencies to provide complete responses at the lowest level of classification possible.

- The Military Departments and Defense Intelligence Agencies will classify each particular data element provided to the IJCSG.

- Originating Authorities will ensure the data has been classified at the appropriate level, with the appropriate caveats.

- All classified responses to both IJCSG data calls and requests for information will be provided using DoD approved secure means.

4.1.1.b Classification IAW original Source Material. Specific information derived from IJCSG data holdings will be classified in accordance with original source material. Proper handling instructions will be identified. Aggregated information derived from IJCSG data holdings will be classified at a minimum at the highest classification of any one source of information.

- The classification of aggregated Defense intelligence-related BRAC data may exceed the highest classification of any one source of information.

- The IJCSG will review all IJCSG generated BRAC data to ensure the proper classification.

- The appropriate DoD approved cover sheet for classified information will be used for classified data. If the material is classified, it will have on top, a classified cover sheet, followed by the OSD BRAC 2005 CLOSE HOLD cover sheet, and then the document. All classified information produced by the IJCSG will be handled and stored in accordance with DoD regulations for classified material.

4.1.1.c Secure Data Storage and Handling Procedures. The IJCSG is unique in regard to other JCSGs, in that it is collecting and analyzing classified information. For this reason, the IJCSG has implemented secure data storage and handling procedures. The IJCSG will collect, aggregate, analyze, and store its data for the BRAC 2005 process up to the TS/SI/TK/G/B/HCS level, as necessary in an appropriately approved, compartmented, standalone computer that is restricted to identified, fully cleared, personnel with a documented "need to know." This computer will be housed in an appropriately approved DoD IJCSGs SCIF.

- The Chair, IJCSG will ensure special security measures are implemented to accommodate special access program (SAP) information. SAP data will be provided directly from the Military Departments and Defense Intelligence Agencies to the Chair, IJCSG. The TIC facility and the Core Team will not store or process any SAP data.

- The Chair, IJCSG has coordinated with each Defense Intelligence community component to ensure all classified data are fully protected in accordance with this SOP, relevant security policies and regulations by requiring the development and DoD IG approval of internal control plans.

4.2 Document Control

The Chair, IJCSG will be responsible for establishing and maintaining an effective document control program for the IJCSG. The IJCSG Security Manager will implement the document control program within the IJCSG SCIF.

4.2.1 Procedures

4.2.1.a Data Storage. All substantive and deliberative information will be stored centrally in the IJCSG SCIF.

4.2.1.b Master Document Registry. A master controlled documents registry will be maintained by the IJCSG Administrative Assistant that indicates the total number of approved copies and the number of copies per approved custodian.

4.2.1.c Document Access List. The IJCSG Administrative Assistant will maintain an access list for the respective centrally stored documents, media, and electronic files. The access list will contain:

- The name of the individual who was provided access to the stored material.
- The individual's organization.
- The specific documents that were accessed.
- The date the information was accessed.

4.2.1.d Access to Documents for People Not on Access List. Individuals (outside the IJCSG Core Team) attempting to access to the information will need the appropriate security clearances, a clearly demonstrated "need to know," and the IJCSG Chair's prior written permission.

4.2.1.e Numbered Copies of Documents. Copies of IJCSG BRAC documents will be numbered and provided to the IJCSG and Core Team members.

4.2.1.f OSD BRAC Cover Sheet. The standard OSD BRAC 2005 CLOSE HOLD cover sheet will protect all hardcopy documentation. All classified and unclassified deliberative documents will be handled appropriate to their markings.

4.2.2 Labeling IJCSG Core Team Documents and Media

To protect the integrity of the BRAC 2005 process, all files, and materials relating to the deliberative process shall be marked appropriately. All documents produced by the IJCSG Core Team shall have the appropriate classification label. Additionally, all deliberative BRAC 2005 documents, including electronic media, will have one of the following statements as header and footer, as appropriate:

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

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

4.3 Certification of Data

The IJCSG's Core Team does not certify data. All data used by the IJCSG Core Team for BRAC 2005 must be certified prior to entering the IJCSG SCIF.

4.3.1 Data forwarded to the IJCSG by the Military Departments or Defense Intelligence Agencies

Data forwarded to the IJCSG by the Military Departments or Defense Intelligence Agencies must be certified by the BRAC process within each particular Military Department and Defense Intelligence Agency.

4.3.2 Data and Information Gathered from External to DoD

Data and information gathered from authoritative or official sources external to DoD need only be certified as to the source if the source's accuracy can be determined by the audit community in accordance with U.S. General Accounting Office guidance.

4.4 Record Keeping

Record keeping is the responsibility of the Chair, IJCSG. Record keeping includes the minutes of meetings, attendance at meetings, distribution lists, status of clearances, Nondisclosure Agreements, and other approved IJCSG documents.

4.4.1 Minutes of Meetings

Minutes will be maintained of all IJCSG meetings. The minutes will contain a record of attendance (Chair, IJCSG will approve attendance at each meeting.), a synopsis of issues discussed, and a discussion of all decisions and recommendations.

4.4.1.a Master Copy of Minutes. The Chair, IJCSG will maintain and store the master copy of classified and unclassified minutes.

4.4.1.b OSD BRAC Copy of Minutes. The OSD BRAC office will retain the original copy of all unclassified minutes.

4.4.1.c Numbered Copy of Minutes for IJCSG Core Team. Numbered copies of the minutes will be provided to the IJCSG Core Team members.

4.4.1.d Minutes of IJCSG Core Team meetings. Minutes are not required for IJCSG Core Team meetings.

4.4.2 Record of Clearances

The IJCSG Security Manager will maintain a current record of all security clearances held by members of the IJCSG Core Team. The IJCSG Security Manager will ensure all personnel assigned to the IJCSG Core Team initiate procedures to maintain their security clearance in an active status.

4.4.3 Nondisclosure Agreements (NDA)

4.4.3.a Responsible for Signing NDA. Each IJCSG member will sign a BRAC 2005 NDA. Additionally, all other individuals working within the process or providing support to the process (including DoD IG, technical experts, contractors, etc.) will be required to sign non-disclosure agreements. (The DoD standard agreement is at Appendix C to "Transformation Through Base Realignment and Closure (BRAC 2005) Policy Memorandum One-Policy, Responsibilities, and Procedures" memorandum). Signing a NDA does not automatically grant access to BRAC data. Copies of Core Team NDAs will be on file in the IJCSG SCIF. The NDA is valid until the Secretary of Defense transmits BRAC recommendations to the Commission and Congress.

4.4.3.b Responsibility for Maintaining File of NDAs. The IJCSG Security Manager will ensure all personnel who access BRAC 2005 material in the IJCSG SCIF have signed a BRAC Non-Disclosure Agreement. The IJCSG Administrative Assistant will maintain a file of all BRAC Non-Disclosure Agreements in the IJCSG SCIF.

4.4.4 Approved BRAC Documents

The IJCSG Security Manager shall ensure all documents are stored IAW standardized DoD procedures, TIC Procedures, and the procedures outlined in this SOP. The IJCSG Administrative Assistant will record, file, and maintain all BRAC approved documents.

4.4.5 IJCSG Core Team Non-Deliberative Notes and Working Papers

IJCSG Core Team members are authorized to maintain personal non-deliberative notes and working papers of Core Team activities in the course of developing IJCSG material. Core Team members are responsible for appropriate markings of all personal notes and working papers.

4.4.6 Information Provided by Technical Experts

Technical expertise may be solicited by the IJCSG to support the development or refinement of analytical products or processes. Technical experts include Intelligence and BRAC Subject Matter Experts, as well as Information Technology and Information System support personnel, as required by either the IJCSG or Core Team. The Military Departments and Defense Intelligence Agencies will identify technical experts to the IJCSG.

4.4.6.a Procedures Related to Technical Experts

- Each technical expert will be briefed on the sensitivity of BRAC data.
- Technical experts will be granted limited access to BRAC 2005 data and information that will allow them to assist the IJCSG in the development and/or refinement of analytical efforts.
- The use of technical experts will be communicated, orally or in writing, to the ISG.

4.4.6.b Certification of Information Provided by Technical Experts. When technical experts provide information, expertise, or data the IJCSG considers relevant and appropriate for analysis, the experts shall submit the information or data in writing with the required certification.

4.5 Access to BRAC 2005 Information

BRAC 2005 data and information shall be treated as sensitive and pre-decisional.

4.5.1 Access for IJCSG Members

The members of the IJCSG have access to all data developed by the IJCSG Core Team and stored within the IJCSG SCIF consistent with the controls set forth in this SOP. The Core Team is responsible for providing preliminary results and analyses to the IJCSG only.

4.5.2 Access for Seniors and Principals

IJCSG Core Team members are authorized to keep seniors apprised of all relevant BRAC activities.

4.5.3 Access for Director, Central Intelligence Agency (DCI) - Community Management Staff (CMS)

A DCI/CMS designated staff representative will be invited to attend IJCSG meetings as an observer. A CMS representative is included as an observer on the Core Team. The

IJCSG Security Manager will ensure security clearances have been passed to the TIC via DIA prior to allowing access to the IJCSG SCIF

4.5.4 Access for Other Approved Recipients. The Chair, IJCSG will make available BRAC information to the following individuals on a need to know basis after the Secretary's recommendations are released on May 15, 2005.

- Chair and Ranking Member of the Senate Armed Service Committee and House Armed Service Committee.
- Chair and Ranking Member of the House Permanent Select Committee on Intelligence and Senate Select Committee on Intelligence.
- Majority and Minority Leaders of the House and Senate.
- Appropriately cleared members of the BRAC Commission.
- Other Recipients approved by the Chair, IJCSG on a case-by-case-basis.

4.5.5 General Accounting Office/Department of Defense Inspector General Audit Access to Records

4.5.5.a Access to Records. Access to records will be as directed by the Chair, IJCSG.

4.5.5.b Copying records. Copying records will be authorized by the Chair, IJCSG.

4.5.5.c IJCSG Core Team Audit Responsibility. Due to the non-deliberative nature of the Core Team's activities, the Core Team has no audit or access responsibilities for the data it produces. DoD IG has an observer member assigned to the Core Team.

4.5.6 Miscellaneous Personnel Requiring Access to the IJCSG SCIF

Access will be granted to other individuals, to include technical experts and outside consultants, only after receiving the consent of the Chair, IJCSG. The IJCSG Security Manager will coordinate the approval process in conjunction with the Core Team Facilitator.

4.6 Dissemination of BRAC 2005 Data

Dissemination of BRAC 2005 data must be authorized by the Chair, IJCSG. Members of the IJCSG must exercise caution to prevent the improper release of and/or access to the BRAC 2005 data. Secure channels will be used for disseminating all classified information.

5.0 PERSONNEL SECURITY

5.1 Security Clearances

All IJCSG members will possess at a minimum a TS/SI/TK/G/B/HCS security clearance. Clearances (collateral and SCI) and accesses must be provided to the TIC Contracting Special Security Officer (CSSO). The TIC will issue a TIC badge, which allows personnel access to the IJCSG SCIF.

5.2 Personnel Approved for Access to the IJCSG SCIF

When opened, the IJCSG SCIF must be occupied by at least one SCI indoctrinated member of the Core Team with at a minimum TS/SI/TK/G/B/HCS accesses. The TIC will issue a TIC badge, which allows personnel access to the IJCSG SCIF. Everyone leaving the IJCSG SCIF is subject to personal and property inspections by the Security Manager/Administrative Assistant.

5.3 Visitors to the IJCSG SCIF

Visitors to the TIC will check in at the TIC Visitor Service Desk located in Suite 100 before access is granted. All visitors must present valid identification (i.e., driver's license, Gov't ID) to the security team member at the Visitor Service Desk. The cleared visitor's identity will then be verified and a visitor badge will be issued. A cleared point of contact must be identified for all uncleared visitors. Foreign national visitors will only be allowed in the TIC with the written authorization of the Chair, IJCSG and Director, DARPA TIC, coordinated thru the appropriate DARPA program manager and with approval of the TIC CSSO. The SCIF TIC badge will be displayed above the waist at all times within the SCIF. All visitors will sign in and out of the BRAC SCIF. Un-sponsored visits are not authorized.

5.3.1 Escorting of Visitors to the IJCSG SCIF

5.3.1.a Categories of Visitors

- **Un-sponsored visitors** are not allowed access to the IJCSG SCIF.
- **Sponsored visitors, with clearances on file,** may be issued NO ESCORT REQUIRED badges.
- **Sponsored visitors, with no clearances on file**, must be escorted by a Core Team member or support person.

5.3.1.b Badges

- **Red Badge.** Indicate the visitor has at least a collateral SECRET clearance. "No escort required" visitors have unescorted access while in the secure perimeter but are restricted to their assigned working room, the restrooms and public corridors.

- **Orange Badge.** Indicates that a TOP SECRET clearance plus SCI accesses, is on file at the TIC.

- **Green Badge.** Indicates that NO Clearance is on file. They require constant visual escort at all times and in all rooms.

5.3.1.c Record Keeping. Authorized visitors will sign in on the visitor log sheet upon entering the IJCSG SCIF.

5.3.1.d Sanitization. Proper sanitization of work areas is critical when uncleared persons are present other than normal duty hours, or when continuous observation of the unclear persons may not be possible. The area will be sanitized prior to any uncleared personnel being granted access to the IJCSG SCIF. Check all desks and tables for visible classified materials.

5.3.1.e Other Associated Escort Procedures

- While escorting uncleared individuals into the SCIF, the escort will ensure personnel are announced as "UNCLEARED PERSONNEL."

- The escort is accountable for the uncleared person(s), as well as any badge(s) issued.

- Visually observe the person(s) under escort at all times.

- Escorts are responsible for inspecting work spaces in advance of uncleared person(s) entering the spaces.

- Core Team members will not discuss classified information in the presence of uncleared person(s).

5.4 Required Notification to Security Manager

5.4.1 Administrative Notifications

The following issues will be forwarded to your SSO and the IJCSG Security Manager/Administrative Assistant:

- Name changes

- Marital status

- Suspicious contacts

- Contacts with representative of a foreign interest
- Foreign travel

5.4.2 Incident Notifications

Report to the IJCSG Security Manager the following incidents:

- Suspected violations of the Security SOP
- Suspected acts of sabotage, espionage, or subversion
- Suspected conditions that threaten the security of SCI information, combinations and passwords
- Suspected mishandling and unauthorized disclosure of classified material
- Suspected compromise, actual compromise, or loss of SCI information or material (SCI material not under visual or physical control of its custodian, or that which cannot be found, will be presumed lost, pending an investigation)
- Observance of physical deficiencies which could reduce the security integrity of the SCIF
- Impending reassignment back to home organization and any new assignments of individuals from your organization to the IJCSG
- Coercion or blackmail attempts that seek to obtain classified information

5.5 Security Education

The IJCSG Security Manager will maintain a security education program to ensure that all SCI-indoctrinated personnel understand the unique sensitivity of the information to which they have access. The security education program will consist of both an initial orientation and continuing security awareness.

5.5.1 Initial Briefing

The initial briefing will include security regulations and requirements, internal SCIF policies, etc.

5.5.2 Continuing Security Education Program

The continuing security education program will support an environment of sharing security awareness material that generally encompass the current DIA and SSO

policies, AIS, and physical security procedures, administrative, and individual classification management.

6.0 CLASSIFIED INFORMATION SECURITY

6.1 Responsibility

The author or drafter of a document is responsible for complying with established security classification guidance and for applying that guidance, including all markings required for its protection, control, and dissemination. Additionally, every person assigned to the IJCSG is responsible for ensuring classified material is properly protected. Finally, working materials, such as drafts and computer disks, shall be protected with the same care as final products.

6.2 Procedures for Marking Classified Documents

The standard classification markings are TOP SECRET, SECRET, and CONFIDENTIAL. Classification and declassification markings will be in accordance with DoD 5200.1R.

6.2.1 Overall Security Classification and SCI Notations

The overall security classification and SCI notations will be marked or stamped, in letters larger and bolder than the text, in a conspicuous location on the document, media, or electronic document.

6.2.2 SCI Control System Caveats

SCI material will be marked with the applicable SCI control system caveat(s) at the bottom of each page of a hard copy document including the front and back covers of the documents. Place the caveat(s) immediately below the classification, centered at the bottom of the page. Use authorized abbreviations to mark portions.

6.2.3 Classification Authority

The classification authority designates the basis for classifications and is either an original or derivative classification authority.

6.3 Transporting Classified Materials

BRAC 2005 documents and data will be safeguarded while being transported from one secure facility to another. Additionally, SCI documents will not be read, studied, displayed, discussed, or used in any manner in public conveyances or places. BRAC 2005 will not be transported outside the local area by couriers; a separate secure means of transportation shall be used.

6.3.1 Courier Procedures

Prior to transporting classified information to or from the IJCSG SCIF, personnel must have the appropriate courier authorizations. The courier's badge, orders, card or letter provides the authority to transport classified information to the level specified on the badge, orders, card or letter within the geographic limits identified. Under no circumstances will couriers exceed limits of their authorization. Courier information must be verified by the IJCSG Security Manager.

6.3.1.a Courier Pouch. SCI material shall be hand-carried using a locked briefcase or pouch as the outer wrapper. An unobtrusive luggage tag shall be attached to the briefcase or pouch which contains the following notation:

PROPERTY OF THE U.S. GOVERNMENT
TO BE RETURNED UNOPENED
(name of organization, telephone number that
will be manned at all times)
AFTER DUTY HOURS TELEPHONE:

6.3.1.b Wrapping Classified Materials

SCI requires double-wrapping. Use two opaque envelopes, kraft wrapping paper, or canvas bags, leather or plastic pouches will preclude observation of the contents. Seal all seams of both wrappers with gummed kraft reinforcing paper tape. Do not use masking or cellophane tape. Include the name of the person or activity for which the material is intended and a receipt for accountability.

- **Inner-Wrapper.** Stamp or print in large letters the address of the agency receiving the document. Stamp or print the appropriate security classification on each side of the inner wrapper (top and bottom). Do not use SCI codeword and caveats on any of the wrapping. Stamp "CONTAINS SENSITIVE COMPARTMENTED INFORMATION."

- **Outer-Wrapper.** Place the address of the receiving organization in the center of the package. Place the outgoing organization in the upper left corner. Secure the outer seams with tape, or other means that protect against surreptitious access.

6.4 Reproduction of Classified Material

6.4.1 Reproduction in the IJCSG SCIF

Unclassified and classified material can be reproduced in the IJCSG SCIF.

Copy only the minimum amount of pages—always for official purposes. (If the document is voluminous, make every effort to obtain a copy from the originator/another source). Ensure the total number of pages copied equates to the total copies intended. Retrieve all copies and originals.

6.4.2 Reproduction of SCI Documents

Reproduction of SCI documents will be kept to a minimum consistent with operational necessity. Copy only the minimum amount of pages—always for official purposes. (If the document is large, make every effort to obtain a copy from the originator/another source). Ensure the total number of pages copied equates to the total copies intended. Retrieve all copies and originals. Double-check the copier machine and the surrounding area for classified material before leaving the area.

6.5 Accountability of Data Call Information

All data call material collected will be controlled. The Security Manager and Administrative Assistant will keep a document receipt for all data call material.

6.6 Secure Terminal Unit (STU-III) and Secure Terminal Equipment (STE)

The Secure Terminal Unit (STU-III) is a controlled cryptographic COMSEC item.
The Secure Terminal Equipment (STE) is not a controlled cryptographic COMSEC item.

6.6.1 Crypton Ignition Keys and KOV-14 Cards

Crypton Ignition Keys (CIK) and KOV-14 cards are unclassified when separated from the STU-III or STE; however, users must protect them from unauthorized use. The CIKs and KOV-14 cards can be left in the STU-III and the STE at all times. If removed, the CIKs and KOV-14 cards can be stored in a GSA-approved security container or a locked file cabinet. When the CIK or KOV-14 card is inserted into STU-III or STE, the terminal is controlled at the same security level as the programmed key. Personnel with access to a keyed unit must have an equal or higher clearance. Every effort must be taken to ensure that the classified information being discussed is properly protected and that all persons hearing the discussion have a need-to-know.

6.6.2 Procedures for STU-III and STE

Before using the STU-III or STE for classified discussions, follow these security practices:

- Does the classification level of the information to be discussed exceed the level identified on the STU-III or STE being used?
- Is the individual cleared to discuss the information?

6.6.2.a Making or receiving a secure call on the STU III

- Put the CIK in the slot on the right side of the STU-III and turn clockwise until you hear a click, if the CIK is not already inserted.

- Dial the telephone number. Once contact is established with the called party and when you are ready, the person initiating the call should press the "Secure Voice" button. The telephone will display "Going Secure". While the STU-III is establishing the secure link, all conversation is blocked.

- Once the secure link is established, the green light in the secure voice window will illuminate and the display will show the HIGHEST common classification and the name of the organization called.

- At the termination of each secure call, make sure that the STU-III goes back to the non-secure mode.

6.6.2.b Making or receiving a secure call on the STE

- Insert the KOV-14 card into the phone if it has not already been inserted and look for the yellow light in the window where it states "card inserted".

- Dial the telephone number. Once contact is established with the called party and when you are ready, the person initiating the call should press the "Secure Voice" button. The telephone will display "Going Secure". While the STE is establishing the secure link, all conversation is blocked.

- Once the secure link is established, the green light in the secure voice window will illuminate and the display will show the HIGHEST common classification and the name of the organization called.

- At the termination of each secure call, make sure that the STE goes back to the non-secure mode.

6.7 IJCSG Secure FAX

6.7.1 Accreditation, Clearances and Documentation

6.7.1.a Accredited for SCI. The secure fax machine is approved and accredited for SCI data transmission.

6.7.1.b Clearances and Need to Know. Individuals transmitting and receiving SCI material must have the appropriate clearance, SCI accesses, and a need-to-know. Always ensure the individual receiving the fax is cleared. Never leave the transmitting

fax machine unattended.

6.7.1.c Control Numbers and FAX Cover Sheet. All FAXs require a control number and a FAX cover sheet.

6.7.1.d Labels and Accountability. All SCI documents transmitted by secure fax will be marked and accounted for in the same manner as hardcopy documents. Individual header or cover sheets used to precede material transmission will be conspicuously marked at the top and bottom with the highest security classification of the transmitted material and any handling caveats.

6.7.2 Procedures for Transmitting a Secure FAX

- Establish STU-III or STE secure voice communication as outlined above. Once "Voice" has been established by the person initiating the call, that same person should press "Secure Data".

- Place documents face down in the secure fax machine.

- After the STU-III or STE shows a green light for secure data, press the START button on the fax machine.

- After transmission is complete, the green "Secure Data" light will extinguish. Confirm with the distant station that they have received a complete fax. Have the other party sign the fax cover sheet stating that all pages were received. The other party will establish a "Secure Data" connection and fax the signed cover sheet back to you. The fax notification form will be held, controlled, and used as a document receipt.

6.7.3 Receiving a Secure FAX

- Answer the phone and verify with the distant station the level of classification and number of pages they are preparing to transmit.

- Establish voice communication and have the person initiating the call press "Secure Voice" and "Secure Data" as outline above.

6.8 Unclassified Telephone

Do not discuss classified information on telephones that are not cleared for classified information and have the following label affix "DO NOT DISCUSS CLASSIFIED INFORMATION.

6.9 Equipment and Media

6.9.1 Accountability of Classified Equipment and Media

All media must be signed in at the TIC front desk. All media or equipment will be controlled according to the highest possible level of information on the media. A Standard Form 711 and applicable SF 706-710 or 712 will be affixed to each piece of magnetic media.

6.9.2 Movement of Classified Equipment and Media

Classified equipment and media will not be removed from the IJCSG SCIFs without IJCSG Security Manager's/Administrative Assistant's approval. The physical movement of such material must be documented with receipts. AIS removal of classified media will be controlled and handled according to collateral and SCI document control procedures.

6.10 Classified Working Papers

Classified working papers are those materials created during preparation of finished documents and material.

- Date when created and mark on the first page the notation "Working Papers - Destroy Within 90 Days."
- Mark the document with the highest classification of any information contained therein; safeguard working materials according to the handling, storage, and disposition requirements for Collateral/SCI.
- Destroy within 90 days of origin or place in control channels.

6.11 Personally Owned Electronic Equipment

6.11.1 Personally Owned Equipment Permitted in the SCIF

Radios, audio and video equipment with only a "playback" feature (no recording capability), or with the "record" feature disabled/removed; electronic calculators, electronic spell-checkers, wristwatches, and data diaries without data ports will be allowed into the SCIF.

6.11.2 Personally Owned Equipment Prohibited in the SCIF

Personally owned photographic, video, audio recording equipment, personally owned computers, palm pilots, cell phones and associated media are prohibited in the IJCSG SCIF.

7.0 DESTRUCTION OF DOCUMENTS AND MEDIA

Both classified and unclassified documents will be destroyed using an approved SEM-

244 cross cut shredder. CD's will be destroyed using a CD Shredder which has been approved by DIA. Trashcans may be used to dispose of paper wrappers, bottles, cans, and like refuse. Newspapers and magazines will either be shredded or disposed of in a separate container from unclassified trash.

8.0 PHYSICAL SECURITY

Physical Security procedures for the IJCSG SCIF are established in accordance with DCID 6/9, "Physical Security Standards for Sensitive Compartmented Information Facilities (SCIF)," 18 November 2002

8.1 Facility Accreditation

8.1.1 IJCSG SCIF Accreditation

SSO DIA/DAC has accredited the IJCSG SCIFs at the TS/SI/TK/G/B/HCS level.

8.1.2 TIC Facility Accreditation

The TIC is accredited through SSO DIA for TS/SI/TK/G/B/HCS.

8.2 TIC Security Provisions

8.2.1 TIC Security Personnel

The security personnel perform a security check within the TIC every two hours, starting about 6:30pm. The security personnel performing this function will be cleared to the collateral SECRET level.

8.2.2 TIC Closed Circuit Television

The TIC SCIF and the IJCSG SCIFs are monitored by a Closed Circuit Television (CCTV) system which is located at the visitor control desk. The CCTV has 2 televisions, and 8 cameras on the lst floor which show the entrance to each hallway and the Rooms including 116 and 117.

8.2.3 TIC Panic Button

A duress button is located at the visitor control desk, which is connected to the Arlington Police.

8.2.4 TIC Alarm System

The alarm system for each room within the TIC SCIF is activated and deactivated by the TIC security personnel. Although the TIC security personnel activate and deactivate the alarms for Room 116 and 117, they do not have the combinations to open the door or

the badge access to Room 116 and 117. The alarm records and tapes will be reviewed each month by the IJCSG Core Team Security Manager/Administrative Assistant.

8.2.5 TIC Corridor Partitions

There are four partitions that have been placed in the hall to separate Rooms 116 and 117 from the other rooms. A table is placed in the hallway between Room 116 and 117 that will be used by the IJCSG Core Team Security Manager/Administrative Assistant to monitor the entrance and exit of the rooms.

8.3 Hours of Operation

The visitor control desk is manned 24 hours a day by personnel cleared to the appropriate level. During normal working hours (8:00am – 5:00pm), the visitor control desk is manned by a security person cleared to the TS/SI level. After duty hours, it is manned by security personnel cleared to the collateral SECRET level.

8.3.1 TIC Duty Hours

8.3.1.a Normal Duty Hours. Monday through Friday from 6:00am – 6:00pm

8.3.1.b After Hours. The TIC visitor control desk must know in advance if you need to work after duty hours or on the weekend. There is a building badge that is needed to gain access to the building, if you will be working in the facility outside normal working hours on a recurring basis, which will be used along with your TIC badge. If you know that you will need access in advance, you can let the visitor control desk know before you leave for the evening and they can notify the person who will be on shift. TIC personnel will be there waiting for your arrival, and you won't need a building badge to get in. The guard will let you in after the proper identification (TIC badge with access level of SCIF). (A copy of the personnel roster (Appendicies A and B) will be maintain by the TIC staff for contacting after duty hours in case of an emergency is located in rooms 116 and 117. Copies of the rosters are given to the Visitor Control Desk for its files.)

8.4 Opening and Closing Procedures for Room 116

8.4.1 Opening Procedures for Room 116

Opening procedures will be posted on the door inside the IJCSG SCIF and in the SOP. These procedures are to be followed by the persons on the access list to open or close the IJCSG SCIF.

- When you arrive to open the IJCSG SCIF, you must inform the person at the security desk that you are going to opening the IJCSG SCIF. They will let you know if the IJCSG SCIF has been opened. If not, they will deactivate the alarm.

- After opening the IJCSG SCIF, annotate the facility security check log on the outside of the door with the time the IJCSG SCIF was opened.
- Flip the OPEN/CLOSED sign to the OPEN position.
- Room 116 does not have to be secured for the day, unless IJCSG Core Team members have departed the building for other locations (i.e. IJCSG Principals meetings at the Pentagon or luncheons).
- There is no two-man rule to open/close room 116.

8.4.2 Closing Procedures for Room 116

Closing procedures will be posted on the door inside the IJCSG SCIF and in the SOP. These procedures are to be followed by the persons on the access list to open or close the IJCSG SCIF. The IJCSG SCIF will be secured by a combination lock at the end of each duty day. The last person shall:

- Ensure all computers are logged off and the monitors are turned off.
- Inspect the room for unsecured classified material. Although open storage is authorized within room 116, good security practices dictate storing materials when practicable. All desktops, safes, bookcases, tables, etc., should be inspected. All classified material that can be secured, should be secured in a safe or other approved security container.
- Ensure all safes are secured by rotating the combination dial at least four complete turns.
- Annotate the SF 702 with the date and time the container was secured.
- Flip the OPEN/CLOSED sign to CLOSED.
- Prior to securing the door for the evening, turn-off all unnecessary lighting.
- Close the door to the room and rotate the combination dial at least four complete turns.
- Double check that the lock is secured by presenting your badge to the card reader and attempting to open the door.
- Annotate the facility security check log on the outside of the door with the time the IJCSG SCIF was secured.
- Flip the OPEN/CLOSED sign to CLOSED.

- Notify the person at the visitor control desk that the room has been locked and secured.

8.5 Procedures for Rooms 117 and 117A

8.5.1 People with access to Rooms 117 and 117A

8.5.1.a Door Combination. All IJCSG Core Team members will have the combination to the room 117. Once opened, IJCSG Core Team members and Oracle will have badge access to room 117. Two people must present/scan their badge, one after another, in order for the door to open after the combination has been dialed.

8.5.1.b Safe Combinations. All IJCSG Core Team members will have access to the safe inside room 117.

8.5.1.c SUN Computer Access. Three Oracle and one IJCSG Core Team Contractor Support personnel will have access to log on to the SUN computer in room 117A.

8.5.2 Opening Procedures for Rooms 117

- Prior to opening room 117, inform the security desk so that the alarm is deactivated.
- After opening the room, two IJCSG Core Team members will annotate the facility security check log on the outside of the door with the time the room 117 was opened.
- Flip the OPEN/CLOSED sign to OPEN.
- Rooms 117 and/or 117A does not have to be secured for the day, unless IJCSG Core Team members have departed the building for other locations (i.e. IJCSG Principals meetings at the Pentagon or luncheons).

8.5.3 Closing Procedures for Rooms 117

Two IJCSG Core Team members will secure room 117. Both individuals will annotate the facility security check log on the outside of the door with the time the SCIF was secured.

- Room 117 is secured by a combination lock and alarm activation at the end of each duty day.
- One Oracle personnel or the IJCSG Contract Support person will ensure that all computers in room 117A computers are logged off and the monitor(s) turned off. All desktops and tables, etc., should be inspected for unsecured classified material.

- Any IJCSG Core Team member will inspect room 117 (including all desktops, tables, etc.) and place any unsecured classified material in the safe. Additionally, ensure the safe is secured by rotating the combination dial at least four complete turns. Annotate the SF 702 with the date and time the container was secured. Flip the OPEN/CLOSED sign to CLOSED.

- Any IJCSG Core Team member will annotate the SF 701 with the date and time the room was checked, turn-off all unnecessary lighting, and close the door to the room. Two IJCSG Core Team members will initiate closing procedures for the door by rotating the combination dial at least four turns, double checking the door to see if it is secured by presenting their badge to the card reader, and attempting to open the door and annotating the facility security check log on the outside of the door with the time the SCIF was secure. Flip the OPEN/CLOSED sign to CLOSED. Notify the facility the visitor control desk that the room 117 has been secured, and request activation of the alarm.

8.6 Emergency Evacuation Plan and Rallying Point

8.6.1 Evacuation Procedure

Every evacuation announcement must be treated as a real evacuation until otherwise CONFIRMED by the Building Manager. Personnel, contractors, and visitors will evacuate the area via the most expedient route as depicted in emergency evacuation signs posted throughout the IJCSG SCIF and TIC. The last person out should check that all areas have been evacuated; terminals logged off and appropriate doors locked or alarmed. **DO NOT WAIT FOR VERIFICATION OF ALARMS.** In all cases, personal safety takes precedence over asset loss or data disclosure. However, security is a primary concern and IJCSG SCIF closing procedures should be performed if time allows. TIC personnel are responsible for ensuring everyone is aware of the evacuation announcement and has left the area.

8.6.2 Rallying Point

The IJCSG Core Team Rallying Point for an Emergency Evacuation is located as shown on the display boards/doors in Rooms 116/117. Proceed out of Rooms 116 and 117, follow the hallway around to your left, you will see an EXIT sign overhead, the door is an emergency exit, follow it out to the ramp and proceed to the rallying point location. Proceed directly to the Rallying Point unless given instructions to do otherwise by Security Manager/Administrative Assistant or the Core Team facilitator.

8.6.3 Accountability

Accountability of personnel will be taken at the point by the Security Manager, Administrative Assistant or the Core Team facilitator. DO NOT leave the area until properly relieved by the Security Manager/Administrative Assistant or the Core Team

Facilitator. The "all clear" will be announced by the TIC Building Manager or by individuals designated by the facility manager.

8.6.4 Security Containers

All of the Security Containers in the IJCSG SCIF are marked with appropriate Priority Levels in case of an emergency.

- **Priority One.** Cryptographic equipment and documents
- **Priority Two. All** operational SCI codeword material, other sensitive intelligence material, and TOP SECRET collateral
- **Priority Three.** Less sensitive administrative SCI material and collateral classified material not included above

8.7 Power Loss and Emergency Power Loss Procedures

The TIC is equipped with a state of the art auxiliary power system. A 10 minute battery back up under full load will come on first, after which a generator will come on and stabilize in 30 seconds from the loss of main power.

9.0 INFORMATION SYSTEM SECURITY

Information Systems (IS) that are used to capture, create, store, process or distribute classified information must be properly managed to protect against unauthorized disclosure of classified information, loss of data integrity, and to ensure the available of the data system. IS are composed of hardware and software. The software breakdown into operating systems (OS), and tools commercial off-the-shelf office and custom applications.

9.1 Responsibilities

9.1.1 IJCSG Security Manager

- The IJCSG Security Manager shall define and document IS security operations procedures for all computer operations.
- The IJCSG Security Manager shall select and procure IS hardware and off-the-shelf applications software. Every effort should be made to select a single set of previously accredited off-the-shelf applications software for use on all desktop computers.

- The IJCSG Security Manager shall coordinate and oversee the accreditation of all hardware and off-the-shelf applications software tools (such as Word, Outlook, Excel, Explorer, etc).

- The IJCSG Security Manager shall arrange for training of all users on procedures.

- The IJCSG Security Manager shall monitor, by spot checking, that all users are proficient in and are utilizing procedures.

- The IJCSG Security Manager shall identify and arrange for the development of unique security operations procedures for all custom applications software to be used by the Core Team and support contractors to accomplish BRAC analyses.

9.1.2 Information Systems Security Manager

The Information Systems Security Manager (ISSM) reports directly to the IJCSG Core Team Facilitator and is responsible for all Oracle automated information system matters within the IJCSG SCIF. The ISSM will also maintain an accurate accountability for all Oracle hardware, software, and contents of the Oracle data base. The ISSM is responsible for developing, implementing, and evaluating the information system security program per NISPOM Chapter 8.

9.1.3 System Users

- System Users shall be accountable for their action on an IS.

- System Users shall ensure that any authentication mechanisms (including passwords) issued for the control of their access to an IS are not shared and are protected at the highest classification level and most restrictive classification.

- System Users shall acknowledge, in writing, their responsibilities for the protection of the IS and classified information.

9.2 Custom Applications Software

Custom Application Software will permit the input of a classification level for all data elements. Additionally, it will automatically prepare and put a classification level equal to the highest classification level of any data used in the preparation of the report.

9.2.1 Accreditation of Custom Application Software

Software Accredited by appropriate external authorities (to OSD and Core Team staff).

9.2.2 OSD Responsibilities

9.2.2.a Staff Support. OSD will provide the staff with appropriate skills, experience and clearances as well as funding necessary to modify custom applications software when required to meet security requirements.

9.2.2.b Funding Support. OSD will provide the staff with appropriate skills, experience and clearances as well as funding necessary to load data into custom applications software from Agency and Service BRAC certified inputs.

9.2.2.c Operator Support. OSD will provide the staff with appropriate skills, experience and clearances as well as funding necessary to operate custom applications software.

9.2.2.d Security Support. OSD Security Staff will populate Section 3 of Chapter 5 for each Custom Applications Software with a set of security operations procedures for each BRAC custom applications software package.

9.2.3 SUN/ORACLE Capacity Data Call Data Base Computer System Definitions

9.2.3.a Oracle Team – one or more contractors from Oracle Corp. Advanced Programs Group.

9.2.3.b Master database – Oracle 9i database running on Solaris 9 in Room 117A.

9.2.3.c Core Team Laptop – laptop computer loaded with MS Office for presentations to Core Team member's organization.

9.2.3.d Oracle Team Workstation – any of five Windows XP workstations in Room 117A.

9.2.3.e Oracle Local Area Network (LAN) – isolated LAN connecting the master database, Oracle Team workstations, and a printer in Room 117A.

9.2.3.f Oracle Parser – Java utility for extracting responses from MS Word document into master database.

9.2.3.g Core Team – composed of representatives from Military Departments or Defense Intelligence Agencies.

9.3 Data Transfer Procedures

9.3.1 Movement of Questionnaire Data to Master Database

- Responses to the IJCSG Capacity Analysis Data Call are submitted to a respective Core Team member's organization. Core Team member's organization consolidate responses from subordinate organizations into a folder of one or more MS Word documents.

- Each Core Team member's organization submits a folder representing that organization's total response to the IJCSG Capacity Analysis Data Call to the Oracle Team.
- Oracle Team processes a folder using Oracle parser.
- Oracle Team checks parser output for errors and re-processes folder/documents as needed.

9.3.2 Movement of Capacity Data from master database to Room 116 for presentations for Core Team

- Oracle Team formats and extracts data from master database into a report as requested by Core Team. Classification level of the report is an aggregate of the classification and handling requirements of the data.
- Report is moved from master database by Core LAN to Oracle Team workstation #2.
- Report is copied to 250MB Zip disk on Oracle Team workstation #2.
- 250 MB Zip disk is moved by classified pouch from Room 117A to 116 under two-man control.
- Core Team laptop is moved from Room 117A to 116 under two-man control and connected to LCD projector.
- Report is accessed on 250 MB Zip disk from Core laptop for display purposes.
- Core Team laptop and 250 MB Zip disk are returned to Room 117A when presentations are complete.

9.4 Office Automation Systems. TBD

9.5 Capacity Analysis Tool-Spreadsheet Template. TBD

9.6 Military Value Scoring Plan Spreadsheet Template. TBD

9.7 COBRA Costing Tool. TBD

**TBD added as needed based on OSD BRAC Office guidance

10.0 DATA CALL DELIVERY PROCESS

10.1 Organizations Making Delivery

Defense Intelligence Agencies and Military Departments

10.2 Procedures for Receiving Data

10.2.1 Check-in Procedures

The individual(s) from Defense Intelligence Agencies and Military Departments notify the Technology Integration Center (TIC) Visitor Desk to call the DoD Project Core Team at (703) 769-9450/9505. The Defense Intelligence Agencies representative and Military Department representative will not need to sign in since they are here only to drop off the media.

10.2.2 Two-Person Rule for Accepting Data

The DoD Project Core Team members receiving the material must consist of two individuals that have access to open Room 117 and one that has access to the safe (one of the three must be from a different organization).

10.2.3 Document Transmittal Sheet

The Defense Intelligence Agencies representative and Military Department representative will sign a document transmittal sheet releasing the material and one of the three individuals from the DoD Project Core Team will sign a sheet receiving it from the Agencies/Military Departments.

10.2.4 Storage in Secure Container

The data will be taken to Room 117 to be locked in the safe or give to the Oracle personnel for processing. The data will be locked in a safe in Room 117 when not being processed.

11.0 INFORMATION RETENTION, STORAGE, RETRIEVAL, DESTRUCTION

11.1 Approval Procedure. Information retention, storage, search and retrieval, and destruction must be approved by the Chair, IJCSG with coordination of the ICJSG Principals.

11.2 Data Retention. All BRAC 2005 IJCSG information will be retained until April 2006. All data and equipment will be held in accordance with DCIDs, DoD Regulations, and Federal Regulations until it has been determined by those Directives to archive or destroy in accordance with proper procedures.

11.3 Procedural Changes. Any changes in these procedures will be IAW the above regulations and approved by the Chair, IJCSG, in coordination with the IJCSG Principals.

Appendix A
After Duty Hours Recall Roster for Room 116

NAME	ORG	HOME #	CELL #	PAGER #
Lyn Young	USD(I)	(703) 445-1742	(703) 795-1372	
Peter Reif, CDR	DON	(703) 858-9546		
Frank Jones	NGA	(703) 648-2427		
Mike Perrin	NSA	(443) 535-0562	(703) 220-1193	
Colin Sullivan	USD(I)	(703) 519-6147		

Appendix B-1
After Duty Hours Recall Roster for Room 117

NAME	ORG	HOME #	CELL #	PAGER #
Lyn Young	USD(I)	(703) 445-1742	(703) 795-1372	
Rita Nobles, Lt Col	Joint Staff J-2	(202) 545-0322		
Peter Reif, CDR	DON	(703) 858-9546		
Frank Jones	NGA	(703) 648-2427		
Mike Perrin	NSA	(443) 535-0562	(703) 220-1193	
Colin Sullivan	USD(I)	(703) 519-6147		
Wayne Howard	USD(I)	(703) 777-6760	(703) 380-6002	(877) 678-5411
Lisa Stevenson Maj	USAF	(703) 922-6794	(571) 216-6386	
Patrick Conway	DIA	(703) 590-2294	(703) 220-6587	

Appendix B-2
Room 117A Access and Recall for Computer

NAME	ORG	HOME #	CELL #	PAGER #
Sonia Smith	Oracle	(540) 720-2248	(540) 270-6914	
Tad Hays	Oracle		(571) 643-9169	
Dirk Avery	Oracle	(301) 864-2664		
Colin Sullivan	USD(I)	(703) 519-6147		

Appendix C
Sensitive Compartmented Information Control System Identification and/or Markings

A. General. Sensitive Compartmented Information (SCI) is information and materials that require special community controls to include, restricted handling within present and future community intelligence collection programs and their products. These special community controls are formal systems of restricted access established to protect the sensitive aspects of sources, methods and analytical procedures. These controls are identified as follows:

B. SCI Control System Markings

1. SCI materials will be identified and marked with the applicable SCI control system caveat at the bottom of each page of a hard copy document including the front and back covers of the document, if present. The SCI control system caveat will normally be placed either immediately below the classification at the bottom of the page or below, and to the right of the classification.

2. If the material is to be controlled in one SCI control system, either of the following markings may be used:

   a. HANDLE VIA (Name of SCI control system) CHANNEL ONLY (HV__ CO)

   b. HANDLE VIA (Name of SCI control system) CHANNEL ONLY (HV__ CC)

3. If the material is to be controlled in two or more systems, the following marking will be applied: HANDLE VIA (Names of SCI control system) CONTROL CHANNELS JOINTLY ONLY (HV__ CCJ)

Appendix D
Acronyms and Abbreviations

ADT ..... Alarm System
AF ..... Air Force
B ..... Byeman
BRAC ..... Base Realignment and Closure
CCTV ..... Closed Circuit Television
CD ..... Compact Diskette
CIK ..... Crypton Ignition Keys
CMS ..... Community Management Staff
COMSEC ..... Communications Security
CSSO ..... Contractor Special Security Officer
DAC ..... DIA Counterintelligence and Security Activity
DAN..... Document Accountability Number
DARPA ..... Defense Advanced Research Projects Agency
DCI ..... Director of Central Intelligence
DCID ..... Director of Central Intelligence Directive
DIA ..... Defense Intelligence Agency
DoD IG ..... Department of Defense Inspector General
FOIA ..... Freedom of Information Act
G ..... Gamma
GAO ..... General Accounting Office
HCS ..... Human Control System
ICP ..... Internal Control Plan
IJCSG ..... Intelligence Joint Cross Service Group
INFOSEC ..... Information Security
ISG ..... Infrastructure Steering Group
IS ..... Information Systems
IT ..... Information Technology
KOV-14 ..... Fortezza
LAN ..... Local Area Network
LCD ..... Projector
MB ..... Mega Bytes
MS ..... MicroSoft
MZM ..... Company Name
NDA ..... Nondisclosure Agreement
NGA ..... National Geospatial-Intelligence Agency
NRO ..... National Reconnaissance Office
NSA ..... National Security Agency
OPSEC ..... Operations Security
OSD ..... Office of Secretary of Defense
POC ..... Point of Contact
SAP ..... Special Access Program

Appendix D
Acronyms and Abbreviations

SCI ..... Sensitive Compartmented Information
SCIF ..... Sensitive Compartmented Information Facility
SF .....Standard Form
SI .....Special Intelligence
SOP .....Standard Operating Procedure
SSO ..... Special Security Office
STE ..... Secure Terminal Equipment
STU-III .....Secure Terminal Unit
TEMPEST ..... Control of Compromising Emanations
TIC ..... Technology Integration Center
TS ..... Top Secret
USAF ..... United States Air Force
USMC ..... United States Marine Corps
USN .....United States Navy
USD(I) .....Under Secretary of Defense for Intelligence
XP..... Workstation

Appendix E
Emergency Instructions (All Emergencies)

A. IF YOU DETECT A FIRE INSIDE THE TIC SCIF, ROOMS 116, 117 OR 117A

1. **ALERT** fellow workers
2. **CALL** (703) 486-4620 (TIC front desk), if time allows
3. **SECURE** all classified material
4. **EVACUATE** the room

B. IF YOU SMELL SMOKE INSIDE THE SCIF, ROOMS 116, 117 OR 117A

1. **ALERT** fellow workers
2. **CALL** (703) 486-4620 (TIC front desk), if time allows
3. **SECURE** all classified material
4. **EVACUATE** the room

C. IF YOU HAVE A MEDICAL EMERGENCY

CONTACT the TIC front desk (703) 486-4620 – The front desk will call 911 and send for assistance

Appendix F
Nondisclosure Agreement

My duties include work assignments and responsibilities in which I may acquire personal knowledge of or access to information concerning the development of recommendations relating to potential closure or realignment of military installations in the Base Realignment and Closure (BRAC) 2005 process. I understand and agree that it is my duty and obligation to comply with the provisions of this agreement respecting such information, and that my violation of this agreement may result in disciplinary action.

1. I understand that the development of any BRAC 2005 information, written or oral, pursuant to the Defense Base Closure and Realignment Act of 1990, as amended, is an official, sensitive, and deliberative process. "Written" information includes all electronic and hard copy forms of communication. I further understand that the development of such information is not limited to final documents or products, but also includes all draft and feeder documents, briefings and notes, as well as any other related oral or written communication.

2. The public and all levels of federal, state, and local government have a right to expect and trust that the BRAC 2005 process will be conducted objectively and impartially. Any unauthorized disclosure of BRAC information undermines that expectation and trust and is therefore prohibited. Unauthorized disclosures may also constitute a violation of law and DoD or Military Department directives, regulations, instructions, policies, or guidance. I promise not to disclose any BRAC information, except as specifically authorized.

3. I further understand that any document or any other written communication, whether draft or final, is the official property and record of the Department of Defense and shall be retained, disseminated, released, and destroyed in accordance with requirements of law and applicable DoD or Military Department directives, regulations, instructions, policies or guidance.

4. I understand that the provision of this agreement bind me personally until the Secretary of Defense transmits BRAC recommendations to the Commission and Congress even if I am reassigned to other duties or stations, retire, or otherwise cease employment or any contract, agency, or other relationship or association with the Department of Defense.

Signature	Date
Name	Printed Organization

Technology Integration Center (TIC)
Master System Security Plan (MSSP)
Education Checklist

For access to all Information Systems (IS) in the TIC you are required to receive and acknowledge your understanding of the following security precautions.

All IS within TIC spaces require formal Identification and Authentication (I&A). This is initiated with your in processing through TIC Security. A network account will be created providing user access commensurate to the security level and need-to-know your sponsoring agency provides. It is extremely important that your sponsoring agency provide a detailed description of all accesses you require.

- Identification and Authentication

  - ✓ No group authentication is used or authorized within TIC spaces.
  - ✓ Unique User IDs for all TIC IS.
  - ✓ The initial authentication (password) will be created by the TIC System Administrator and must be changed at first log-on. The password is required to have 8 characters and a minimum of one UPPERCASE letter, and one number or special character.
  - ✓ You will be required to update your password every 180 days without repeating a password for six sessions.
  - ✓ Access will expire if your account is not created within 60 days of initialization or if you fail to update your password within the established 60 days.
  - ✓ After 6 months without use, your account will be removed from the network. Program Manager approval will be required to reestablish your account.
  - ✓ After 3 unsuccessful log-on attempts your account will be "locked out". The TIC System Administrator will need to be contacted in order to "unlock" your account.
  - ✓ Reauthentication will be required after the system you are logged onto has remained inactive for 15 minutes.
  - ✓ Letting another person use your account after you logon with your User ID is prohibited. Access to any network within the TIC requires a unique User ID and password.
  - ✓ Simultaneous logon of two or more systems on the same network is prohibited.

- Hardware and Software

- ✓ All magnetic media (e.g., floppy disks, 4mm or 8mm tapes, removable hard drives, etc.) and related equipment (monitors, CPUs, keyboards, etc.), classified and unclassified, will be under the direct control of the TIC CSSO/ISSM. Magnetic media and related equipment entering or exiting the TIC will be processed using SIMS through TIC Security (Room 106) or the Visitor Service Desk (Room 100). The magnetic media and/or equipment will have an accountability number assigned and be logged into the TIC by type and title. At no time will personal magnetic media and/or equipment be brought into the TIC unless specifically authorized by the TIC CSSO/ISSM. If personally owned magnetic media and/or equipment are accidentally brought into the SCIF area, it will remain in the TIC and controlled as though classified.

- ✓ MP3 players are not authorized in SCIFs.

- ✓ Personally created CD-ROMs/DVDs containing data/music, and commercially procured music CD-ROMs/DVDs are not authorized for use in Government computer systems.

- ✓ In order to protect TIC systems from malicious code, all files must be checked for viruses before introduction. The use of public domain software is strongly discouraged. The TIC CSSO/ISSM must approve each installation of public domain software.

- ✓ All material printed from IS will be properly classified, receipted from TIC personnel, logged and safeguarded, commensurate to the security classification of the document.

- ✓ Where classified and unclassified information are processed on collocated IS, unclassified information will be marked. All unmarked material will be considered the classification level of accreditation.

- ✓ Personnel in rooms where keyboard/video/mouse (KVM) or keyboard/monitor/mouse (KMM) switches are in use, must adhere to the following responsibilities:

  - Protect the IS and KVM/KMM in your area.
  - Report any "spillage" of classified information in accordance with the JDCSISSS.
  - Safeguard and report any unexpected or unrecognized computer output, including both displayed or printed products in accordance with Joint DoDIIS/Cryptologic SCI Information Systems Security Standards (JDCSISSS) regulation
  - Use different passwords on each system connected through a KVM/KMM.
  - Ensure that each systems screen lock displays the classification level and that the password is required to regain entry to the system.
  - Ensure that the systems screen lock is invoked if the system is left unattended of if there is a 15-minute period of inactivity for each system.
  - Mark/maintain all magnetic media IAW Chapter 13 of JDCSISSS.

- Configuration Management

  Applies a level of discipline and control to the processes of system maintenance and modification and provides system users with a measure of assurance that the implemented system represents the approved system.

  ✓ Baseline and Terminal Configuration Change Logs are maintained on all TIC IS.

  ✓ All changes, additions, and deletions to hardware and/or software configurations require coordination with and approval of the TIC CSSO/ISSM or Facility Manager. Hardware and/or software baseline documentation will be updated when the network or terminal is upgraded or a new version of installed software is approved/installed for use. The System Administrator will perform all upgrades (hardware or software), after approval by the TIC CSSO/ISSM. The System Administrator will update the TIC Terminal Configuration Change Log for each hardware or software configuration change.

- Network Audit Capability

  Security auditing involves recognizing, recording, storing, and analyzing information related to security-relevant activities. Audit records are used to determine which activities occurred and which user or process was responsible.

  All systems are setup to automatically create and maintain audit records. System audit records are created to document the following:

  - Date and time of action, the system locale of the action, the system entity that initiated or completed the action, the resources involved, and the action involved.
  - Successful and unsuccessful log-ons and log-offs.
  - Successful and unsuccessful accesses to security-relevant objects and directories, including creation, open, close, modification, and deletion.
  - Changes in users through authenticators.
  - Denial of access resulting from an excessive number of unsuccessful log-on attempts.

  ✓ Audit trail contents are only available to System Administrators and ISSM personnel and are not able to be modified or deleted.

  ✓ Audit records are retained for at least one review cycle or as required by the sponsoring agency.

- Backup and Restoration

  The regular backup of information is necessary to ensure users have continuing access to the information.

- ✓ All essential and security-relevant information, including software tables and settings, such as router tables, software, and documentation, are backed-up per the MSSP.

- ✓ Incremental backups are performed daily (Monday-Thursday with a full backup being performed on Friday and the last operational day of each month).

Your signature indicates that you understand and comply with the TIC MSSP as addressed above. This familiarization brief must be signed annually after initial indoctrination.

To view the complete MSSP contact the ISSM or CSSO, 703-486-4620.

Printed Name: _____

Signature: _____ Date: _____

TIC Staff: _____

Signature: _____ Date: _____

ACTIVITY SECURITY CHECKLIST

DIVISION/BRANCH/OFFICE	ROOM NUMBER	MONTH AND YEAR
	116	

Irregularities discovered will be promptly reported to the designated Security Office for corrective action.

Statement

I have conducted a security inspection of this work area and checked all the items listed below.

TO *(If required)*	FROM *(If required)*	THROUGH *(If required)*

ITEM	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
1. Security containers have been locked and checked.																															
2. Desks, wastebaskets and other surfaces and receptacles are free of classified material.																															
3. Classified Material have been properly stored.																															
4. TV has been turned off.																															
5. Copier has been turned off.																															
INITIAL FOR DAILY REPORT																															
TIME																															

ACTIVITY SECURITY CHECKLIST

DIVISION/BRANCH/OFFICE	ROOM NUMBER	MONTH AND YEAR
	117	

Irregularities discovered will be promptly reported to the designated Security Office for corrective action.

Statement

I have conducted a security inspection of this work area and checked all the items listed below.

TO *(If required)*	FROM *(If required)*	THROUGH *(If required)*

ITEM	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
1. Security containers have been locked and checked.																															
2. Desks, wastebaskets and other surfaces and receptacles are free of classified material.																															
3. Classified Material have been properly stored.																															
INITIAL FOR DAILY REPORT																															
TIME																															

SECURITY CONTAINER CHECK SHEET

TO (if required)	THRU (if required)

CERTIFICATION

I CERTIFY, BY MY INITIALS BELOW, THAT I HAVE OPENED, CLOSED OR CHECKED THIS SECURITY CONTAINER IN ACCORDANCE WITH PERTINENT AGENCY REGULATIONS AND OPERATING INSTRUCTIONS.

MONTH/YEAR

DATE	OPENED BY		CLOSED BY		CHECKED BY		GUARD CHECK (if required)	
	INITIALS	TIME	INITIALS	TIME	INITIALS	TIME	INITIALS	TIME

FOLD HERE - REVERSE FOLD FOR FULL USE OF BOTH SIDES - FOLD HERE

SECURITY CONTAINER CHECK SHEET

FROM	ROOM NO.	BUILDING	CONTAINER NO.

CERTIFICATION

I CERTIFY, BY MY INITIALS BELOW, THAT I HAVE OPENED, CLOSED OR CHECKED THIS SECURITY CONTAINER IN ACCORDANCE WITH PERTINENT AGENCY REGULATIONS AND OPERATING INSTRUCTIONS.

MONTH/YEAR

DATE	OPENED BY		CLOSED BY		CHECKED BY		GUARD CHECK (if required)	
	INITIALS	TIME	INITIALS	TIME	INITIALS	TIME	INITIALS	TIME

STANDARD FORM 702 (8-85) (EG)
Prescribed by GSA/ISOO
32 CFR 2003
Designed using Perform Pro, WHS/DIOR, Jul 94

FACILITY SECURITY CHECK LOG

MONTH & YEAR	ORGANIZATION	SAFE/ROOM/DOOR NUMBER

The individual certifies with his/her initials and time that all closing procedures have been carried out in accordance with the standard practices and procedure for the location indicated above.

DATE OF MONTH	UNLOCKED BY		LOCKED BY		CHECKED BY	
	TIME	INITIALS	TIME	INITIALS	TIME	INITIALS

CLASSIFIED DOCUMENT ACCOUNTABILITY RECORD

For use of this form, see AR 380-5; the proponent agency is the Office, Assistant Chief of Staff for Intelligence.

DATE

SECTION A - GENERAL

TO:	FROM:

DATE RECEIVED	ACTION OFFICE(S)	SUSPENSE DATE(S)	REGISTER OR CONTROL NO.

CONTROL LOG OR FILE NO.	CLASSIFICATION	NUMBER OF COPIES	DESCRIPTION *(Type, File Ref., Unclassified Subject or Short Title and Number of Indorsements/Incls)*	DATE OF DOCUMENT	ORIGINATOR

SECTION B - ROUTING

TO	COPY NO.	DATE	I ACKNOWLEDGE RECEIPT OF THE MATERIAL DESCRIBED HEREON	
			PRINTED NAME	SIGNATURE
1.				
2.				
3.				
4.				
5.				

SECTION C - DESTRUCTION CERTIFICATE *(Check appropriate block)*

MATERIAL DESCRIBED HEREON HAS BEEN:

☐ DESTROYED ☐ TORN IN HALF AND PLACED IN A CLASSIFIED WASTE CONTAINER *(AR 380-5)*

PAGE OR COPY NO

OFFICE SYMBOL	DATE	PRINTED NAME OF CUSTODIAN OR REP	SIGNATURE
DESTRUCTION RECORD NO.	DATE	PRINTED NAME OF CERTIFYING/DESTR. OFF.	SIGNATURE
PAGE OR COPY NUMBER	DATE	PRINTED NAME OF WITNESSING OFFICIAL	SIGNATURE

SECTION D - REPRODUCTION AUTHORITY

NUMBER OR COPIES TO BE REPRODUCED	AUTHORIZED BY	DATE

SECTION E - RECEIPT/TRACER ACTION *(Check appropriate block)*

☐ RECEIPT OF DOCUMENT(S) ACKNOWLEDGED ☐ DOCUMENT(S) HAVE NOT BEEN RECEIVED

☐ TRACER ACTION: SIGNED RECEIPT FOR MATERIAL DESCRIBED ABOVE HAS NOT BEEN RECEIVED.

DATE	PRINTED NAME, GRADE OR TITLE	SIGNATURE

COMMENTS

CLASSIFICATION

DoD PROJECT CORE TEAM
Classified Fax Number: (703) 521-2606
Unclassified Fax Number: (703) 271-4049

FAX TRANSMITTAL SHEET

TO: _____ FROM: _____

OFFICE: _____ OFFICE: _____

FAX NUMBER: _____ FAX NUMBER: _____

OFFICE NUMBER: _____ OFFICE NUMBER: _____

COMMENTS: _____

_____

_____

TRANSMITTED BY: _____ DATE: _____

HEADER + _____ PAGE(S)

CLASSIFICATION