

**REQUEST FOR RECORDS DISPOSITION AUTHORITY**  
 (See instructions on reverse)

LEAVE BLANK	
JOB NO.	N1-457-89-2
DATE RECEIVED	
NOTIFICATION TO AGENCY	
In accordance with the provisions of 44 U.S.C. 3303a the disposal request, including amendments, is approved except for items that may be stamped "disposal not approved" or "withdrawn" in column 10.	
7/25/89 Date	 Archivist of the United States

TO: GENERAL SERVICES ADMINISTRATION,  
 NATIONAL ARCHIVES AND RECORDS SERVICE, WASHINGTON, DC 20408

1 FROM (AGENCY OR ESTABLISHMENT)

NATIONAL SECURITY AGENCY

2. MAJOR SUBDIVISION

INFORMATION RESOURCES MANAGEMENT

3. MINOR SUBDIVISION

OFFICE OF HISTORY AND ARCHIVES

(b)(3)

6. CERTIFICATE OF AGENCY REPRESENTATIVE

I hereby certify that I am authorized to act for this agency in matters pertaining to the disposal of the agency's records; that the records proposed for disposal in this Request of \_\_\_\_\_ page(s) are not now needed for the business of this agency or will not be needed after the retention periods specified.

A Request for immediate disposal.

B Request for disposal after a specified period of time or request for permanent retention.

C. DATE (b)(3)

(b)(3)

7. ITEM NO.

RECORDS RELATING TO INFORMATION SECURITY

53 ITEMS TOTAL  
 6 ITEMS PERMANENT

PERMANENT MEDIA IS PAPER

CLASSIFIED JOB FILE RETAINED AT NSA INCLUDES APPRAISAL MEMO DATED 6/15/89

PERMANENT SERIES WILL BE TRANSFERRED TO THE NATIONAL ARCHIVES AFTER 50 YEARS IF DECLASSIFIED.

SERIES STILL CLASSIFIED AFTER 50 YEARS WILL BE RE-REVIEWED EVERY 10 YEARS UNTIL DECLASSIFIED.

~~TOP SECRET~~



**NSA RECORDS DISPOSITION  
SCHEDULE FOR  
C  
INFOSEC APPLICATIONS AND NATIONAL  
COMPUTER SECURITY CENTER**

M-457-89-2

~~HANDLE VIA COMINT CHANNELS ONLY~~  
~~TOP SECRET~~

~~TOP SECRET~~



**NSA RECORDS DISPOSITION**

**SCHEDULE FOR**

**C**

**INFOSEC APPLICATIONS AND NATIONAL**

**COMPUTER SECURITY CENTER**

~~HANDLE VIA COMINT CHANNELS ONLY~~  
~~TOP SECRET~~

~~TOP SECRET~~

NSA/CSS  
RECORDS DISPOSITION SCHEDULE  
FOR  
C  
INFOSEC STANDARDS  
AND  
EVALUATIONS

~~HANDLE VIA COMINT CHANNELS ONLY~~

~~TOP SECRET~~

# UNCLASSIFIED

## INTRODUCTION

### NSA RECORDS DISPOSITION SCHEDULES

#### WHAT ARE RECORDS DISPOSITION SCHEDULES?

Records disposition schedules provide for the proper disposition of an agency's records. Schedules list and describe the records generated by a Federal agency and provide guidance on how long records are to be maintained. As defined in 44 USC 30 "records" include all books, papers, maps, photographs, machine readable materials, or other documentary materials regardless of physical form or characteristic made or received by an agency of the United States Government under Federal law or in connection with the transaction of public business. Federal law mandates that the head of each agency submit to the Archivist of the United States record schedules proposing the disposition of that agency's records. The schedules provide for the prompt destruction of temporary records and for the permanent retention and preservation of records which illustrate and document the organization, functions policies, decisions, procedures, operations, or other activities of the agency, or which contain informational data of an historical nature.

#### WHY NSA HAS RECORDS DISPOSITION SCHEDULES

NSA's Records Disposition Schedules are designed to provide for and to simplify the appropriate disposition of Agency records and to aid Agency officials in gaining intellectual control over the increasing amount of information generated by the Agency. Designed to reflect the records actually produced, used, or stored by each Agency Key Component, the proper application of these schedules will ensure that NSA complies with the Federal Records Act, the Privacy Act, and the Freedom of Information Act. Furthermore, the schedules, if properly implemented, will provide a cost effective, efficient management program for the Agency's information by drastically reducing duplication and the unnecessary storage of paper records.

Traditional schedules have dealt with records on a generic basis. In general, these schedules concentrated on paper records and ignored or dismissed the growing volume of electronically produced and stored information. Consequently, most schedules quickly became dated and virtually unusable as the records described in the schedules and the records maintained in agency offices did not correspond. The new schedules attempt to remedy these problems by identifying and describing in detail the specific records of each Key Component. The schedules reflect all records, - paper, micro-

UNCLASSIFIED

## UNCLASSIFIED

form or electronically generated - compiled, used, or maintained by each Key Component. They are uniquely designed for each Key Component.

### WHAT INFORMATION IS CONTAINED IN THE SCHEDULES?

Each schedule contains a list of the data bases or files generated or used by each Key Component. The description of each data base or file includes:

1. the title
2. a narrative description of the contents
3. the inclusive date span of the information contained in the data base or file
4. the physical location
5. the storage media
6. the volume of material created or held by the office per year (for paper files the volume is given in cu. ft., for data bases the volume is given in sectors, tracks, or the number of characters)
7. the highest classification of the inclusive material
8. the approved disposition
9. the disposition number.

For data bases the description also includes information on the hardware and the software required to run them.

### HOW TO USE THE SCHEDULES

For the proper disposition of a data base or file locate the appropriate office in the Table of Contents, identify the data base or file, and apply the approved disposition. If a file is permanent retire it to the NSA Archives using the disposition number from the schedule. If you have records that are scheduled for destruction you may retire them to the NSA Records Center prior to their destruction date and the Records Center will handle the disposition or you may dispose of them yourself at the appropriate time. Records retired to the NSA Records Center must have a specific destruction date. If the schedule does not indicate a specific date call the NSA Records Center and the T54 staff will provide one. For the disposition of records not covered by the schedules contact T54, The Office of Archives and Records, and fill out a Standard Form 115.

The schedules are produced in loose leaf form to facilitate changes as they occur in the record keeping practices of the offices. New pages will reflect additions, deletions, or changes in the descrip-

UNCLASSIFIED

## UNCLASSIFIED

tion and will be issued periodically. Future generations of the schedules will be available on-line with updates made by the Key Components following approval by T54 and the National Archives. This will ensure greater accuracy and currentness.

### HOW TO RETIRE RECORDS

In order to retire noncurrent records - paper, microform, or audio-visual, to the NSA Records Center for temporary or permanent storage the office records monitor needs to follow the following procedures.

(1) Call the Records Center (972-2295) to ascertain if storage space is presently available and to receive a unique accession control number for the material being retired.

(2) Prepare a triplicate Form 02295 for each series of records being retired. The office records monitor must assure that the proper disposition number from the Records Disposition Schedule is noted on the form. Please follow those instructions carefully. One form should be prepared for each series of records being retired.

(3) Follow the proper procedures for forwarding classified materials.

(4) Deliver to nearest NSA mail center for forwarding to the NSA Records Center via the NSA courier service.

Retirement requirements for special records (audio-visual, microform, electronic) are different because of the perishability of the media. The Code of Federal Regulations requires that permanent microform records be stored on silver halide process microform. A master copy of permanent audio-visual records (video tapes, audio tapes, etc.) should be sent as soon as possible to the NSA Archives to ensure their preservation. Permanent text files stored on floppy disks should be printed out in hard copy before retirement to the NSA Archives. The NSA Archives is at present not equipped to handle electronic records. Current handling procedures (SAB 3, OPI) should be followed in the interim.

### REFERENCE SERVICE ON RETIRED RECORDS

Retired records are held in the NSA Records Center for the period of time prescribed in the NSA Records Disposition Schedules. During this period the records are available for loan or reference. Permanent records will be held indefinitely by the NSA Archives.

UNCLASSIFIED

## UNCLASSIFIED

They will be processed and made available for Agency reference purposes upon their arrival at the NSA Archives. After 30 years T54 archivists will review them and remove duplicative and extraneous materials. Requests for loans of retired records may be made by telephone or in writing to T541. The requester should know the accession control number as shown in Form 02295 in order to request records. The loan period is 30 days. Records may also be reviewed at the NSA Records Center by appointment.

### USEFUL INFORMATION

#### THE UNLAWFUL REMOVAL OR DESTRUCTION OF RECORDS

Federal law requires the Director of the National Security Agency to establish safeguards against the unlawful removal or loss of agency records, and to make known to NSA personnel the penalties provided for the unlawful removal or destruction of such records. 44 USC 3106 provides that the Director, with the assistance of the Archivist of the United States, initiate action through the Attorney General for the recovery of records believed to be unlawfully removed from the Agency. 44 USC 3314 also states that no records of the United States Government may be altered or destroyed except as stipulated under 44 USC Chapter 31. Penalties for the willful and unlawful destruction, damage, or alteration of Federal records are stipulated in the U.S. Criminal Code (18 USC 2071)n.

#### OFFICIAL AND PERSONAL RECORDS

Records and papers of a private or nonofficial nature which pertain only to an individual's personal affairs but are maintained in a Federal office must be clearly designated as nonofficial and will at all times be filed and maintained separately from the official records of the office. In cases where matters requiring the transaction of official business are received in private correspondence, the portion of such correspondence pertaining to official business must be extracted and made a part of the official record. The definition of official records includes any materials generated or received in pursuance of Federal law or in connection with the transaction of public business. Correspondence designated "personal," "private," etc., but which pertains to the conduct of public business, is an official record subject to the provisions of Federal law. Official records are public records and belong to the office not the individual.

Questions regarding Agency records, official records, the schedules, or the transfer of records to the NSA Archives should be ad-

UNCLASSIFIED

**UNCLASSIFIED**

dressed to T54, The Office of Archives and Records.

**UNCLASSIFIED**

# UNCLASSIFIED

## CONTENTS

### TITLE

Introduction

NSA Mission Statement

### INFOSEC STANDARDS AND EVALUATIONS

C Mission Statement

#### C Records

- C Staff Subject File
- Executive Subject File
- Chief Scientist Subject File
- Chief C Travel and Briefing File
- Correspondence File
- Special Assistant Correspondence File
- Deputy Chief's Subject File
- C Personnel File
- Administrative File

### C09 ADMINISTRATIVE AND MANAGEMENT STAFF

C09 Mission Statement

#### C09 Records

- Administrative Subject File
- Technical Library Reports
- Reference File
- Retired Records Identification File
- Vital Records Identification File
- Element Top Secret Control File
- Library Card File

### C6 INFOSEC EVALUATION TECHNOLOGIES

C6 Mission Statement

#### C6 Records

- Office Correspondence and Suspense Logs File

### C603 INTERDISCIPLINARY SECURITY EVALUATION TECHNOLOGIES STAFF

C603 Mission Statement

C603 Records

UNCLASSIFIED

# UNCLASSIFIED

## C61 CRYPTOMATHEMATICS SECURITY EVALUATION TECHNOLOGIES

C61 Mission Statement

C61 Records

    Cryptosecurity Assessment File  
    COMSEC Analysis Reports File

## C62 COMPUTER SCIENCE SECURITY EVALUATION TECHNOLOGIES

C62 Mission Statement

C62 Records

    Braille Books  
    Personal Records and Suspense Log

## C63 ENGINEERING AND PHYSICAL SCIENCES SECURITY EVALUATION TECHNOLOGIES

C63 Mission Statement

C63 Records

    Correspondence File  
    Research Reports

## C64 SECURITY EVALUATION LABORATORY AND COMPUTING SUPPORT

C64 Mission Statement

C64 Records

    Research and Analysis File  
    TEMPEST Reports  
    NSA Standards of Acceptance File  
    Office Correspondence File

## C7 INFOSEC DEVELOPMENTAL SYSTEMS EVALUATIONS

C7 Mission Statement

C7 Records

    Administrative File  
    Personnel File  
    Correspondence File

UNCLASSIFIED

# UNCLASSIFIED

C71 TRUSTED PRODUCTS AND NETWORK SECURITY EVALUATIONS

C71 Mission Statement

C71 Records

- Software Evaluation Manuals
- Evaluation File
- Product Evaluations Forum Subsystem Data Base
- Vendor File
- MITRE Support File
- MINSTREL File

C72 TACTICAL, KEY MANAGEMENT, AND NATO/FOREIGN SYSTEMS EVALUATIONS

C72 Mission Statement

C72 Records

- Research and Analysis File
- COMSEC Equipment File
- ADPS Reports Control Case Folders
- C72 Personnel Files
- Chronological Correspondence Files
- Administrative Communications Files
- C721 Personnel Files
- C722 Personnel Files
- Project Information Files
- Cryptogeneration File

C73 SPACE, WEAPONS, TRANSEC SIGNALS AND STRATEGIC SYSTEMS  
SECURITY EVALUATIONS

C73 Mission Statement

C73 Records

- Correspondence File
- Personnel File

C74 IMPLEMENTATIONS SECURITY

C74 Mission Statement

C74 Records

- Daily Correspondence File
- SFA/TEMPEST/CV File
- Implementation Evaluation Reports and Technical Notes File
- PDB TOOL File

UNCLASSIFIED

# UNCLASSIFIED

Weekly Items File  
Monthly Activity Report File  
Clearance File

## C75 SECURITY GUIDANCE

C75 Mission Statement

### C75 Records

Cryptosecurity Assessment File  
Administrative Communications File  
Personnel Information File  
C75 Memoranda File  
Weekly Items of Interest File  
Information File  
C Technical Literature Award File  
Clearances File  
Business Developmental Council File

## C76 ADVANCED TECHNOLOGY AND FUTURE SYSTEM SECURITY GUIDANCE

C76 Mission Statement

### C76 Records

Administrative File  
Personnel File  
Correspondence File  
Technical Library File

## C8 INFOSEC STANDARDS, ASSESSMENTS, AND SYSTEM SERVICES

C8 Mission Statement

### C8 Records

Administrative File

## C81 STANDARDS, CRITERIA AND GUIDELINES

C81 Mission Statement

### C81 Records

TNI Comments Data Base  
DBMS Guideline Forum Data Base  
Trusted UNIX Data Base  
TNI Discussion Data Base  
TNI Interpretations Data Base

UNCLASSIFIED

# UNCLASSIFIED

TNG Data Base

C82 RISK ASSESSEMENT AND THREAT MODELS

C82 Mission Statement

C82 Records

Technical Assessment File  
Administrative File

C83 SYSTEM SERVICES

C83 Mission Statement

C83 Records

Graphics Library System Data Base  
Mailing and Conference Systems (MACS) Data Base  
Administrative File  
Purchase Request File  
Honeywell Multics Operational Systems Instruction File  
Network Users Administrative File

C9 INFOSEC FIELD EVALUATION

C9 Mission Statement

C9 Records

TEMPEST Advisory Group Subject File  
Administrative File

C903 INFOSEC FIELD EVALUATION SENIOR TECHNICAL STAFF

C903 Mission Statement

C903 Records

C91 FIELDDED INFOSEC SYSTEM AND NETWORK EVALUATION

C91 Mission Statement

C91 Records

Travel Data Base  
Reports File  
Correspondence File  
T Operating System File  
Suspense Log Data Base

UNCLASSIFIED

# UNCLASSIFIED

C92 COMSEC MONITORING AND ANALYSIS

C92 Mission Statement

C92 Records

- Administrative File
- Procurement Request File
- Signals File
- Operations File
- SIGSEC Technical Analysis Report File
- Adversary SIGINT Targeting Data Base
- Assessment Data Base
- Equipment Data Base

C93 FACILITIES AND COUNTERMEASURES EVALUATION

C93 Mission Statement

C93 Records

- Countermeasures Development File
- Technical Security Evaluation File
- Correspondence File
- NSA/SCIF TEMPEST Program File

C94 POLICY, PLANNING, AND MANAGEMENT SUPPORT

C94 Mission Statement

C94 Records

- Subject File
- National TEMPEST Information Center Library
- Administrative File
- Threat File
- Technical File
- Program/Project File

UNCLASSIFIED

**UNCLASSIFIED**

**NATIONAL SECURITY AGENCY  
CENTRAL SECURITY SERVICE  
NSA/CSS**

**UNCLASSIFIED**

~~TOP SECRET~~

NATIONAL SECURITY AGENCY/CENTRAL SECURITY SERVICE

CREATION AND AUTHORITY

Pursuant to the Presidential directives of 24 October 1952, which declare that Communications Intelligence (COMINT) and Communications Security (COMSEC) are national responsibilities, the Department of Defense established, by directive, the National Security Agency to succeed the Armed Forces Security Agency. The National Security Council added Electronic Intelligence (ELINT) to NSA's national mission in 1958.

In accordance with Presidential directives and pursuant to the National Security Act of 1947, the National Security Council issued National Security Council Intelligence Directive (NSCID) No. 9, dated 29 December 1952, and the National COMSEC Directive, dated 20 October 1953, which defined the NSA COMINT and COMSEC missions respectively. ELINT functions were first recognized in NSCID No. 17, dated 16 May 1955. The original COMINT and ELINT directives were superseded by and combined into NSCID No. 6, "Communications Intelligence and Electronics Intelligence," dated 15 September 1958. NSCID No. 6 was updated on 17 February 1972 and retitled "Signals Intelligence." The COMSEC directive of 1953 was updated on 25 April 1957, on 26 August 1968, and again on 20 June 1979. The SIGINT and COMSEC directives name the Secretary of Defense as executive agent for the conduct of SIGINT and COMSEC activities and direct that the SIGINT and COMSEC missions be carried out in response to guidance from the National Foreign Intelligence Board (NFIB) and the National Communications Security Committee (NCSC), respectively.

In accordance with the provisions of NSCID No. 6, the Secretary of Defense established the Central Security Service (CSS) under the Director, NSA. The Secretary of Defense provided for the National Security Agency/Central Security Service (NSA/CSS) by promulgating DoD Directive S-5100.20 dated 23 December 1971. He approved the NSA/CSS Organization Plan on 14 April 1972 to implement that directive. The NSA/CSS is a separately organized agency within the Department of Defense under the direction, authority, and control of the Secretary of Defense. It is subject to the provisions of Department of Defense directives and procedures to the extent that they are applicable and consistent with its missions and functions. Major components of the NSA/CSS are the National Security Agency (NSA) and the Service Cryptologic Elements (SCEs) of the Military Departments. Under the NSA/CSS, SIGINT resources are unified but decentralized. The NSA is the management, operational tasking, analytical and production arm of the system and the SCEs are the field

~~HANDLE VIA COMINT CHANNELS ONLY~~

~~TOP SECRET~~

~~TOP SECRET~~

arm. The Director, NSA/Chief, CSS exercises operational control of the collection effort through the Deputy Chief, CSS and the SCE Commanders. The NSA operates a number of special field collection facilities, but the primary field collection effort is conducted by the SCEs.

In January 1983, the Secretary of Defense approved having the Director, NSA, perform the collateral duty of Director, Joint Special Studies Group (JSSG). The Director, JSSG is responsible for conducting classified studies under the direction of the Joint Chiefs of Staff.

In September 1984, NSDD-145 expanded the authority of the Secretary of Defense as the Executive Agent of the Government for COMSEC to include telecommunications and automated information systems security. NSDD-145 established the Director, NSA as the National Manager to act as the operating arm of the Executive Agent.

#### PURPOSE

The resources of the National Security Agency/Central Security Service are organized for the accomplishment of two national missions:

a. The Signals Intelligence (SIGINT) mission is to provide an effective, unified organization and control of all SIGINT collection and processing activities of the United States, and to produce SIGINT in accordance with objectives, requirements, and priorities established by the Director of Central Intelligence with the advice of the National Foreign Intelligence Board.

b. The Information Security (INFOSEC) mission encompasses two major activities: (1) The Communications Security (COMSEC) mission is to implement protective measures to deny unauthorized persons national security-related, including sensitive but unclassified, information derived from telecommunications and to also prevent these persons from disrupting or causing the deception of such communications. Measures included within COMSEC are cryptosecurity, transmission security, emissions security, physical security, and technical security. (2) The Computer Security (COMPUSEC) mission is to implement protective measures designed to prevent deliberate or inadvertent unauthorized access, disclosure, acquisition, manipulation, modification, or loss of information contained in automated systems used within the Department of Defense, other Government Agencies and the private sector. DoD Directive 5215.1, dated 25 October 1982, established the DoD Computer Security Evaluation Center (CSEC), provided policy, and assigned responsibilities for the technical evaluation of computer system and network

~~HANDLE VIA COMINT CHANNELS ONLY~~

~~TOP SECRET~~

~~TOP SECRET~~

security, and related technical research.

#### ORGANIZATION

The Director, NSA/Chief, CSS is assisted in the management and direction of NSA/CSS by a principal Deputy Director, NSA, and a Deputy Chief, CSS. His organization includes seven Deputy Directors for specific functional areas, two Assistant Directors, a Chief of Staff, an Inspector General, a General Counsel, a Chief Scientist, and the Director's Senior Council.

~~HANDLE VIA COMINT CHANNELS ONLY~~  
~~TOP SECRET~~

**UNCLASSIFIED**

**C**  
**INFOSEC STANDARDS**  
**AND**  
**EVALUATIONS**

**UNCLASSIFIED**

## INFOSEC STANDARDS AND EVALUATIONS

The Chief of C is responsible to the DDI as the Security Evaluation Authority for U.S. INFOSEC systems. As such, he is responsible for the security evaluation and assessment of the COMSEC, COMPUSEC and TECHSEC measures in information systems processing or communicating classified and sensitive information within NSA, DOD and related contractor facilities, and other U.S. Government organizations. He is also responsible for evaluating commercially available computer security products; setting standards, criteria, and specifications; conducting evaluation research; and providing security guidance for such measures. In addition, he provides appropriate technical leadership and guidance to U.S. and foreign governments in related COMSEC, COMPUSEC and TECHSEC areas.

---

Primary functions include:

[NSA25X6]

1. Providing security evaluation and risk assessment of specific INFOSEC products, equipments, systems, applications, and facilities in development and in the field, and evaluating the resistance of cryptoalgorithms to cryptanalytic attack.
2. Conducting interdisciplinary and cryptomathematical research to develop and modify attacks and to develop hardware and software evaluation tools designed to discover vulnerabilities in INFOSEC systems.
3. Prescribing security standards for trusted computer systems, cryptographic equipments, technical security countermeasures, and computer and information systems.
4. Performing COMSEC monitoring, signals, and traffic analysis to support the evaluation and assessment of INFOSEC equipments/systems.
5. Providing security guidance/requirements to developers.
6. Assessing the security level of computer hardware/software products that have general utility and for placement on the Evaluated Products List; and providing computer security advice to the vendors.
7. Developing threat models and risk assessment models.

**FOR OFFICIAL USE ONLY**

8. Managing, operating and maintaining the NCSC computer and network facilities.
9. Providing overall technology, architecture design, program development, engineering development, acquisition and life cycle support planning and related support to the Technical Security Engineering and Evaluation Program.
10. Managing and operating the Information Security Laboratory.
11. Responsible for the overall technical health of the organization and of the constituent disciplines.

**FOR OFFICIAL USE ONLY**

UNCLASSIFIED

C Staff Subject File

This file contains C Staff Subject files concerning pertinent operational matters, projects under the purview of C, and Key correspondence involving the organization as well as correspondence files.

DATE SPAN: 1985 to Present  
LOCATION: C  
STORAGE MEDIA: Paper  
VOLUME: 4 cu. ft.  
CLASSIFICATION: TOP SECRET  
DISPOSITION: Permanent. Transfer to NCRC when 5 years old.  
DISPOSITION NO.: C-1

Executive Subject File

This is the subject file for the Executive, C Group.

DATE SPAN: 1988 to Present  
LOCATION: C  
STORAGE MEDIA: Paper  
VOLUME: 10 cu. ft.  
CLASSIFICATION: TOP SECRET CODEWORD  
DISPOSITION: Retain by OPI until no longer required for operations.  
DISPOSITION NO.: C-2

PENDING CHANGES:

C-1 thru C-8 —  
may be old C

X1-1 thru X1-3  
X2-1 thru X2-10

transferred to  
C but not yet  
claimed

UNCLASSIFIED

# UNCLASSIFIED

## Chief Scientist Subject File

This file contains the subject file for the Chief Scientist (C Group).

DATE SPAN: 1987 to Present  
LOCATION: C  
STORAGE MEDIA: Paper  
VOLUME: 2 cu. ft.  
CLASSIFICATION: TOP SECRET  
DISPOSITION: Retain by OPI until no longer required for operations.  
DISPOSITION NO.n C-3

## Chief C Travel and Briefing File

This file contains records concerning Chief C's meetings and visits, including TDYs.

DATE SPAN: 1985 to Present  
LOCATION: C  
STORAGE MEDIA: Paper  
VOLUME: 6 cu. ft.  
CLASSIFICATION: SECRET  
DISPOSITION: Retain by OPI until no longer required for operations.  
DISPOSITION NO.: C-4

UNCLASSIFIED

Correspondence File

This is a chronological record of correspondence from C Group.

DATE SPAN: 1985 to Present  
LOCATION: C  
STORAGE MEDIA: Paper  
VOLUME: 2 cu. ft.  
CLASSIFICATION: SECRET  
DISPOSITION: Permanent. Transfer to NCRC after 2 years.  
DISPOSITION NO.: C-5 001A-1

Special Assistant Correspondence File

This file contains incoming and outgoing letters, memoranda, reports, and other records reflecting the work of the C Special Assistant.

DATE SPAN: 1987 to Present  
LOCATION: C  
STORAGE MEDIA: Paper  
VOLUME: 10 cu. ft.  
CLASSIFICATION: TOP SECRET  
DISPOSITION: Destroy when 5 years old.  
DISPOSITION NO.: C-6

**FOR OFFICIAL USE ONLY**

# UNCLASSIFIED

## Deputy Chief's Subject File

This file contains the Deputy Chief's (C) subject and project files.

DATE SPAN: 1985 to Present  
LOCATION: C  
STORAGE MEDIA: Paper  
VOLUME: 2 cu. ft.  
CLASSIFICATION: TOP SECRET CODEWORD  
DISPOSITION: Retain by OPI until no longer required for operations.  
DISPOSITION NO.: C-7

## C Personnel File

This file contains descriptions, performance appraisals, awards, and background information for all personnel in C Group.

DATE SPAN: 1985 to Present  
LOCATION: C  
STORAGE MEDIA: Paper  
VOLUME: 10 cu. ft.  
CLASSIFICATION: CONFIDENTIAL  
DISPOSITION: Destroy 1 year after separation or transfer of employee from C Group. (GRS 1-18a)  
DISPOSITION NO.: C-8

UNCLASSIFIED

# UNCLASSIFIED

## Administrative File

This file includes records covering such general office administration subjects as travel, awards, personnel, security, training, and budgets.

DATE SPAN	1985 to Present
LOCATION	C
STORAGE MEDIA	Paper
VOLUME	
CLASSIFICATION	TOP SECRET NOFORN
DISPOSITION	Cut off annually. Destroy when 3 years old or when no longer needed, whichever is sooner. (GRS 23-1)
DISPOSITION NO.	C-9

UNCLASSIFIED

C09  
ADMINISTRATIVE  
AND  
MANAGEMENT STAFF

**FOR OFFICIAL USE ONLY**

Management and Administrative Staff

The Chief, C09, is responsible to the Chief, C, for recommending, implementing and monitoring manpower and administrative policies and programs, management procedures, resources management, facilities, recruitment, COMSEC equipment and controlled item accountability, and maintaining the technical library.

Primary functions include:

1. Advising the Chief, C, and serving as a focal point for implementing administrative actions. Advising and assisting in the formulation and execution of management and administrative policies and procedures.
2. Maintaining the C Table of Distribution and providing administrative services pertaining to all personnel actions.
3. Administering the C recruitment program.
4. Providing a central point of authority within C Group for formulating and monitoring execution of the C Group Program Budget.
5. Providing guidance and assistance to C Group managers in the documentation and management of their acquisition programs. Providing final review of the procurement requests prepared by the Group to ensure the acquisition process is in accordance with DOD and Agency regulations.
6. Monitoring the expenditure of awards, travel, training, and overtime allocations.
7. Directing and managing career development and enhancement programs, such as evaluations, training, promotions, awards, etc.
8. Maintaining a technical library, which serves as the office of record for ISSO equipment and system evaluations.
9. Maintaining a central registry/action tracking system for all C Group actions and correspondence.

10. Providing security guidance and reporting.

**FOR OFFICIAL USE ONLY**

# UNCLASSIFIED

## Administrative Subject File

This file contains records pertaining to budgets, maintenance, personnel, security, space, training, travel and related administrative matters.

DATE SPAN: 1986 to Present  
LOCATION: C09  
STORAGE MEDIA: Paper  
VOLUME: 12 cu. ft.  
CLASSIFICATION: TOP SECRET NOFORN  
DISPOSITION: Cut off annually. Destroy when 3 years old or when no longer needed, whichever is sooner. (-GRS 23-1)  
DISPOSITION NO.e C09-1

## Technical Library Reports

This file consists of technical reports pertaining to cryptologics, cryptoequipments, and information security systems. Included are logics which have never been used as well as logics, equipment, and systems with wide deployments. Details of cryptanalytic weaknesses and attacks are discussed; these documents are extremely sensitive.

DATE SPAN: 1940 to Present  
LOCATION: C09  
STORAGE MEDIA: Paper  
VOLUME: 33 cu. ft.  
CLASSIFICATION: TOP SECRET CODEWORD NOFORN  
DISPOSITION: Permanent. Transfer to NCRC when no longer needed for operations.  
DISPOSITION NO.e C09-2

UNCLASSIFIED

Reference File

This file consists of copies of Agency Standard Regulations, Directives, Circulars, Manuals and related records.

DATE SPAN: 1960 to Present  
LOCATION: C09  
STORAGE MEDIA: Paper  
VOLUME: 3 cu. ft.  
CLASSIFICATION: TOP SECRET CODEWORD NOFORN  
DISPOSITION: Destroy when superseded or no longer needed for operations. *002 B-2*  
DISPOSITION NO.: C09-3

Retired Records Identification File

This file contains a listing of records retired to the NSA/CSS Records Center, including Forms 02295 and 02295A (Retired Records Listing).

DATE SPAN: 1950 to Present  
LOCATION: C09  
STORAGE MEDIA: Paper  
VOLUME: 1 inch  
CLASSIFICATION: UNCLASSIFIED  
DISPOSITION: Destroy when related records are destroyed and when no longer needed for operations.  
DISPOSITION NO.: C09-4

**FOR OFFICIAL USE ONLY**

# UNCLASSIFIED

## Vital Records Identification File

Files documenting records forwarded to the Agency Vital Records Depository, including Form 1295 (Transmittal of Material) and Form A70B (Transmittal of Controlled Material).

DATE SPAN: 1950 to Present

LOCATION: C09

STORAGE MEDIA: Paper

VOLUME: 1 inch

CLASSIFICATION: UNCLASSIFIED

DISPOSITION: Destroy when related records are destroyed or returned (no longer to be stored as Vital Records) or when no longer needed for operations.

DISPOSITION NO.: C09-5

## Element Top Secret Control File

These records are controlled by Element Top Secret Control Officers. They consist of cards, listings, covering material internal to NSA/CSS. Documents requiring limited distribution outside NSA/CSS are assigned to the Agency-wide Control System.

DATE SPAN: 1952 to Present

LOCATION: C09

STORAGE MEDIA: Paper

VOLUME: 2 cu. ft.

CLASSIFICATION: TOP SECRET CODEWORD NOFORN

DISPOSITION: Place records in inactive file upon downgrading, destruction, or transfer of related items. Destroy one year thereafter.

DISPOSITION NO.: C09-6

UNCLASSIFIED

UNCLASSIFIED

~~Library Card File~~ \*

~~This file contains cross-referenced 5" x 8" cards that provide abstracted information from Agency technical reports. (The reports are stored in the Technical Library.) This file will be duplicated in electronic form.~~

~~DATE SPAN:~~ 1940 to Present

~~LOCATION:~~ C09

~~STORAGE MEDIA:~~ Paper, hard disk

~~HARDWARE:~~ SUN

~~VOLUME:~~ 6 cu. ft.

~~CLASSIFICATION:~~ TOP SECRET CODEWORD NOFORN

~~DISPOSITION:~~ A. Paper Copy: Permanent. Transfer to NCRC when no longer needed for operations.

~~B. Electronic Copy: Delete or destroy when no longer needed for operations.~~

~~DISPOSITION NO.:~~ C09-7 A and B

\*~~Obsolete. No longer created.~~ See 6/12/2014 email.

MPB

UNCLASSIFIED

**C6**  
**INFOSEC**  
**EVALUATION**  
**TECHNOLOGIES**

**FOR OFFICIAL USE ONLY**

C6

Information Systems Security (INFOSEC) Evaluation Technologies

The Chief, C6, is responsible to the Chief of C for the research and development of techniques, technologies, instrumentation and tools for application in the security evaluation and assessment of INFOSEC (including COMSEC, COMPUSEC and TECHSEC) measures, equipments and systems in design, under development and fielded.

e

the

performance and management of interdisciplinary research to support the evaluation process, the establishment and maintenance of evaluation laboratory facilities as well as requisite computer resources, and support for the development of INFOSEC standards, criteria and guidelines. Furthermore, C6 is responsible for maintaining centers of technical expertise to provide evaluations and to support the evaluation process as well as the ISSO in the areas of mathematics, cryptanalysis, computer science, and engineering and physical sciences. Finally, C6 is responsible for maintaining an awareness of INFOSEC/SIGINT equity issues and providing technical support in that arena.

Primary functions include:

1. Developing, maintaining and enhancing techniques, technologies, instrumentation and tools used by INFOSEC evaluators in the performance of their evaluation, verification, analysis and exploitation responsibilities. Oversee and manage this function throughout the INFOSEC Evaluation Organization.
2. Maintaining and fostering centers of technical expertise in the areas of mathematics, cryptanalysis, computer science, and engineering and physical sciences by conducting basic, applied and interdisciplinary research in support of INFOSEC evaluators and evaluations.
3. Developing mathematical and cryptanalytic techniques and attacks applicable to the system evaluation process, evaluate the security of cryptographic algorithms, and providing mathematical and cryptanalytic support to the INFOSEC Evaluation Organization as well as the ISSO.
4. Developing COMPUSEC techniques and technologies, and providing technical security support for evaluators and

evaluations in the areas of assurance, modeling, formal methods and methodology, vulnerability analysis, penetration testing, software and hardware verification and analysis, networks and communications protocols analysis.

5. Developing TECHSEC protection techniques and technologies, and providing technical security support for evaluators and evaluations in the areas of detection technology, protective packaging technology, and in the development of adversarial techniques, countermeasures and state-of-the-art instrumentation.
6. Providing state-of-the-art evaluation laboratory facilities (including signals, computer, and TECHSEC) and computing resources for the INFOSEC Evaluation Organization.
7. Maintaining and fostering technical liaison and exchanges with other agency and non-agency elements, organizations and centers of technical expertise engaged in scientific disciplines applicable to the support of evaluators and evaluations. Also, foster awareness throughout the INFOSEC Evaluation Organization as well as the ISSO of the state-of-the-art in these scientific disciplines through publications, training, seminars, and attendance at conferences.

**UNCLASSIFIED**

\*Office Correspondence and Suspense Logs File

This file contains office correspondence and suspense logs.

DATE SPAN: 1990 to Present

LOCATION: C6

STORAGE MEDIA: Paper/Magnetic Disk

VOLUME: 10 file folders

CLASSIFICATION: TOP SECRET CODEWORDN

DISPOSITION: Close annually. Transfer hard copy to the NCRC. Delete or destroy after 3 years or sooner if no longer required for operations. (GRS 23-1)

DISPOSITION NO.: C6-1

**UNCLASSIFIED**

C603  
INTERDISCIPLINARY  
SECURITY  
EVALUATION  
TECHNOLOGIES  
STAFF

**FOR OFFICIAL USE ONLY**

~~CONFIDENTIAL~~

C603

Interdisciplinary Security Evaluation Technologies Staff

The mission of C603 is to foster the improvement of techniques, technologies, instrumentation, and tools used by the INFOSEC Evaluation Organization, and to initiate the development of others as needed.

Primary functions include:

1. Serving as a focal point within C6 to determine the techniques, technologies, instrumentation, and tools requirements of the INFOSEC Evaluation Organization and to assist in establishing priorities for their development.
2. Maintaining awareness of available techniques, technologies, instrumentation and tools in industry, the National Laboratories, Federally Contracted Research Centers, other Government agencies (including Second Parties), and the Agency itself (especially the R&D Organization's Tech Base Program).
3. Performing and encouraging others to perform research activities, especially of an inter-disciplinary nature, which will lead to potentially useful techniques, technologies, instrumentation, and tools for evaluation of and establishment of standards for INFOSEC systems.
4. Disseminating information about new techniques, technologies, instrumentation, and tools throughout the INFOSEC Evaluation Organization through publications, briefings, seminars, and conferences.
5. Maintaining awareness of and coordinating tool development activities throughout the INFOSEC Evaluation Organization.

~~CONFIDENTIAL~~

C61  
CRYPTOMATHEMATICS  
SECURITY  
EVALUATION  
TECHNOLOGIES

**FOR OFFICIAL USE ONLY**

NSA25X6

C61

Cryptomathematics Security Evaluation Technologies

[redacted] cryptographics algorithms, developing new cryptanalytic techniques, conducting basic and applied research in support of its evaluation function, and applying general cryptomathematics techniques in support of other (non-algorithmic) evaluations.

Primary functions include:

1. Developing the theory of mathematical cryptanalysis relevant to INFOSEC cryptographyn
2. Developing cryptanalytic techniques and attacks applicable to algorithms (including algorithms implemented in software)e
3. Evaluating the susceptibility to, or resistance of, such algorithms to cryptanalytic attack, and accurately establishing the costs of these attacks against both typical and worst-case usagen
4. Prescribing standards for judging when an enemy might decide to carry out a given cryptanalytic attackn
5. Consulting with Agency cryptanalytic elements for the purposes of sharing INFOSEC cryptanalytic knowledge and acquiring knowledge of potentially useful techniques and results developed elsewhere; conducting close liaison with IDA/CCR ] [redacted]

[PL 86 36/50 USC 3605]

[redacted] and performing other external liaison as required, including second partyn

6. Determining the requirements for cryptanalytic theory and techniques that are needed for the evaluation of other aspects of INFOSEC systems. Promote the use of and support the application of these techniquesn

## Cryptosecurity Assessment File

This file includes evaluation and analysis records generated by NSA analysts regarding cryptosecurity assessment.

DATE SPAN: 1973 to Present  
LOCATION: C61  
STORAGE MEDIA: Paper  
VOLUME: 10 cu. ft.  
CLASSIFICATION: TOP SECRET CODEWORD NOFORN  
DISPOSITION: Permanent. Transfer to NCRC when no longer needed for operations.  
DISPOSITION NO.: C61-1

## COMSEC Analysis Reports File

This file contains analytical studies of U.S. and allied communications.

DATE SPAN: 1981 to Present  
LOCATION: C61  
STORAGE MEDIA: Paper  
VOLUME: 30 cu. ft.  
CLASSIFICATION: TOP SECRET CODEWORD NOFORN  
DISPOSITION: Permanent. Transfer to NCRC when no longer needed for operations.  
DISPOSITION NO.: C61-2

**FOR OFFICIAL USE ONLY**

C62  
COMPUTER SCIENCE  
SECURITY  
EVALUATION  
TECHNOLOGIES

**FOR OFFICIAL USE ONLY**

~~CONFIDENTIAL~~

C62

### Computer Science Security Evaluation Technologies

C62 is responsible for supporting the security evaluation of INFOSEC products and systems. The mission of C62 is to perform research and development activities which advance evaluation techniques, technologies, tools and procedures. The primary focus will be on the application of computer science and computer security to the system development, evaluation and certification processes.

Primary functions include:

1. Developing and maintaining expertise in computer science, computer security, and other related areas which are essential to the development and analysis of modern INFOSEC systems.
2. Developing requirements for evaluation technologies needed to analyze the security of cryptographic algorithms, hardware, software, communications protocols, systems, and networks.
3. Identifying techniques to improve the efficiency, degree of assurance, and thoroughness of the security evaluation process. Ensuring that appropriate evaluation technology is available for use by INFOSEC analysts.
4. Researching system design and implementation weaknesses which can be exploited using the disciplines of computer science and computer security.
5. Researching and developing multi-disciplinary techniques, technologies and tools for the security evaluation of hardware, software, protocols, systems, and networks.
6. Interfacing with organizations involved in the development and application of system security technology including C603, C7, C9, R2, V, the National Laboratories, and others.

~~CONFIDENTIAL~~

# UNCLASSIFIED

## Braille Books

This file contains braille manuals covering subjects such as math, statistics, and computer programming.

DATE SPAN: 1968 to Present

LOCATION: C62

STORAGE MEDIA: Paper

VOLUME: 1 cu. ft.

CLASSIFICATION: SECRET

DISPOSITION: Destroy when no longer needed for operationsn

DISPOSITION NO.n C62-1

UNCLASSIFIED

# UNCLASSIFIED

## ~~CANDLESNUFFER Data Base \*~~

~~This data base contains information documenting the development of software analysis COMPUSEC tools through the use of advanced programming techniques. Reports are sent to the Technical Library.~~

~~DATE SPAN: Under development~~

~~LOCATION: C62~~

~~STORAGE MEDIA: Paper, machine listings~~

~~HARDWARE: Mainframe (CONSEL)~~

~~SOFTWARE: Under development~~

~~VOLUME: 1 cu. ft.~~

~~CLASSIFICATION: SECRET~~

~~DISPOSITION: Delete or destroy when two years old or when no longer needed for operations, whichever is later.~~

~~DISPOSITION NO.s C62-2~~

~~DELETED: 20 NOV. 1991~~

\*~~Obsolete. No longer created.~~ See 6/12/2014 email  
MPB

UNCLASSIFIED

**UNCLASSIFIED**

\*Personal Records and Suspense Log

This file contains the personal records and suspense log for C62.

DATE SPAN: 1989 to Present

LOCATION: C62

STORAGE MEDIA: Paper

VOLUME: 2 file folders

CLASSIFICATION: TOP SECRET CODEWORD

DISPOSITION: A. Civilian Personnel File- Destroy 1 year after separation or transfer of employee. (GRS 1-18a)  
B. Other Materials- Destroy after 3 years or sooner if no longer required for operations. (GRS 23-1)

DISPOSITION NO.n C62-3 A and B

**UNCLASSIFIED**

C63  
ENGINEERING  
AND  
PHYSICAL SCIENCES  
SECURITY  
EVALUATION  
TECHNOLOGIES

**FOR OFFICIAL USE ONLY**

C63

Engineering and Physical Sciences  
Security Evaluation Technologies

C63 is responsible for the development of techniques, technologies, instrumentation and tools that support technical security evaluators and evaluations, develop new attack techniques, detect the presence of technical security attacks, develop countermeasures for providing both the protection against technical security attacks and the protection of INFOSEC equipment and keying materials, and develop program to protect against the tampering with and the modification of INFOSEC equipment.

Primary functions include:

1. Developing engineering and physical science techniques, technologies, instrumentation and tools for application to INFOSEC systems evaluations.
2. Characterizing and identifying technical security attacks and countermeasures for INFOSEC products, hardware, systems and facilities.
3. Developing new technologies to provide tamper protection and positive authentication of INFOSEC systems during their production, shipment and use; including the development of anti-reverse engineering techniques for IC's.
4. Developing new tools and techniques to advance the state-of-the-art in inspection capability for INFOSEC systems.
5. Developing technical security signal acquisition and analysis capabilities for application to both laboratory and field evaluations.
6. Interfacing with other organizations involved with the development and application of technical security technology including C9, R9, Y26, the National Laboratories and other government organizations.

## Correspondence File

This file contains incoming and outgoing correspondence and memoranda related to C63's general office administration.

DATE SPAN: 1986 to Present  
LOCATION: C63  
STORAGE MEDIA: Paper, magnetic disk  
HARDWARE: IBM AT and Xerox Star  
SOFTWARE: Proprietary  
VOLUME: .25 cu. ft.  
CLASSIFICATION: TOP SECRET NOFORN  
DISPOSITION: Destroy when 3 years old or when no longer needed for operations, whichever is sooner. (GRS 23-1)  
DISPOSITION NO: C63-1

## Research Reports

This file contains technical security research reports concerning technology, methods, techniques and defensive countermeasures related to technical security.

DATE SPAN: 1986 to Present  
LOCATION: C63  
STORAGE MEDIA: Paper  
VOLUME: 1 cu. ft.  
CLASSIFICATION: TOP SECRET NOFORN  
DISPOSITION: Permanent. Transfer to NCRC when no longer needed for operations.  
DISPOSITION NO: C63-2

**FOR OFFICIAL USE ONLY**

C64  
SECURITY EVALUATION  
LABORATORY  
AND  
COMPUTING SUPPORT

**FOR OFFICIAL USE ONLY**

C64

Security Evaluation Laboratory and Computing Support

C64 is responsible for providing, managing, and maintaining advanced computing and office automation support, signals collection and analysis capability, and state-of-the-art laboratory facilities for the INFOSEC Evaluation Organization.

Primary functions include:

1. Providing for the planning, budgeting, procurement, installation, maintenance, managing, and disposal of computer and office automation resources required by the INFOSEC Evaluation Organization, particularly in the areas of super-computing, office automation, and networking.
2. Providing technical support for the INFOSEC Evaluation Organization's computing resources which include, but are not limited to, CRANIUM, LOGICV, CONSEL, CALFHOOD, and FENCING.
3. Establishing state-of-the-art evaluation laboratory facilities.
4. Providing for the planning, budgeting, procurement, installation, maintenance, managing, and disposal of the INFOSEC Evaluation Organization's laboratory resources.
5. Providing technical support for the users of the INFOSEC Evaluation Organization's laboratory facilities and resources.
6. Providing signals analysis support to INFOSEC evaluators and laboratory resources for the collection, processing, displaying, and analysis of signals of interest to the INFOSEC Evaluation Organization.

Research and Analysis File

This file includes records documenting research and analysis efforts in evaluation, assessment, and math techniques. Included are records documenting program management.

DATE SPAN: 1969 to Present  
LOCATION: C64  
STORAGE MEDIA: Paper  
VOLUME: 40 cu. ft.  
CLASSIFICATION: TOP SECRET CODEWORD NOFORN  
DISPOSITION: Permanent. Transfer to NCRC when no longer needed for operations.  
DISPOSITION NO. C64-1

~~TEMPEST Reports \*~~

~~This file includes reports of TEMPEST tests by contractors, other government agencies, the military services, private industry, and NSA elements.~~

~~DATE SPAN: 1980 to Present  
LOCATION: C64  
STORAGE MEDIA: Paper  
VOLUME: 30 cu. ft.  
CLASSIFICATION: TOP SECRET NOFORN  
DISPOSITION: Destroy when no longer needed for operations or when they become obsolete. (002C)  
DISPOSITION NO.: C64-2~~

\*Obsolete. No longer created. See 6/12/2014 email. MPB

**FOR OFFICIAL USE ONLY**

**UNCLASSIFIED**

NSA Standards of Acceptance File

This file includes documentation on security fault analysis and cryptographic standards for equipment.

DATE SPAN: 1969 to Present  
LOCATION: C64  
STORAGE MEDIA: Paper  
VOLUME: 30 cu. ft.  
CLASSIFICATION: TOP SECRET CODEWORD NOFORN  
DISPOSITION: Permanent. Transfer to NCRC when no longer needed for operations.  
DISPOSITION NO. ~~B~~ C64-3

\*Office Correspondence File

This file contains correspondence.

DATE SPAN: 1989 to Present  
LOCATION: C643  
STORAGE MEDIA: Paper  
VOLUME: 16 cu. ft.  
CLASSIFICATION: TOP SECRET CODEWORD  
DISPOSITION: Close annually. Destroy after 3 years. (GRS 23-1)  
DISPOSITION NO.: C64-4

**UNCLASSIFIED**

*C7*  
INFOSEC  
DEVELOPMENTAL  
SYSTEMS  
EVALUATIONS

**FOR OFFICIAL USE ONLY**

C7

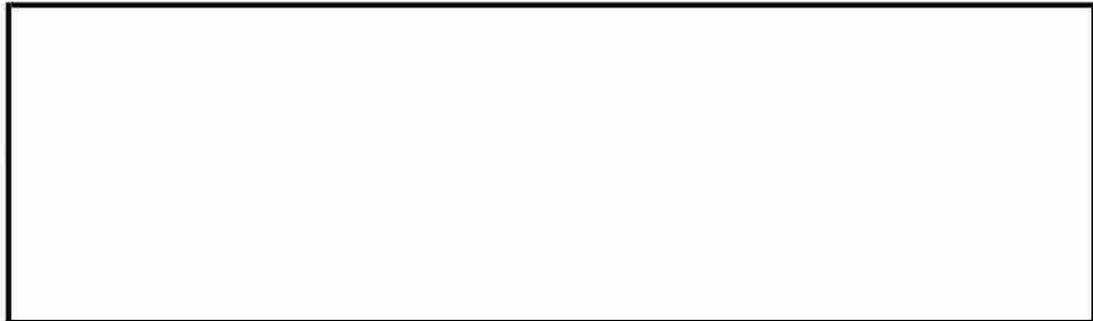
INFOSEC Developmental Systems Evaluations

The Chief, C7, is responsible to the Chief of C: as the source of security evaluation and security guidance support to information security product development organizations; as a major participant in C efforts in security criteria and standards and the performance of security assessments; as a major participant in C efforts in advancement of security technologies and evaluation tools; in supporting field evaluations and research phase evaluations with information and expertise; and for maintaining the expertise and leadership needed for all of the above.

Primary functions include:

1.

NSA25X6



2. Providing security guidance for the development, implementation and application of such systems and products. Security guidance will be promulgated in part by:
  - a. assisting in establishing and specifying tailored Functional Security Requirements Specifications;
  - b. advising or assisting in correcting noted deficiencies;
  - c. providing technical support to system acquisition authorities in the selection, design, implementation and evaluation of hardware, software, and procedural security methods and techniques; and
  - d. providing guidance on trusted product developments via the Vendor Assistance Program.
3. Participating in research applicable to the secure development, implementation, application, and evaluation

of systems.

4. Documenting, publishing and disseminating (as appropriate) system security evaluations and research results.
5. Participating in the performance of security assessments, recommending the approval and operational use of systems, based upon satisfactory security evaluation.
6. Establishing and maintaining technical liaison with all appropriate organizations both internal and external to ISSO/NSA.

# UNCLASSIFIED

## \*Administrative File

This file contains information concerning promotions, awards, billets, and vacancy announcements. There are local travel claims and TDY requests for all of C7, as well as information on all NCS courses, withdrawals, external training and executive development training.

DATE SPAN: 1989 to Present

LOCATION: C7

STORAGE MEDIA: Paper

VOLUME: 3 cu. ft.

CLASSIFICATION: TOP SECRET CODEWORD NOFORN

DISPOSITION: Destroy after 3 years or when no longer required for operations. (GRS 23-1)

DISPOSITION NO.: C7-1

## \*Personnel File

This file contains information on each C7 individual (a personnel file on each.)

DATE SPAN: 1990 to Present

LOCATION: C7

STORAGE MEDIA: Paper

VOLUME: 2 cu. ft.

CLASSIFICATION: TOP SECRET CODEWORD NOFORN

DISPOSITION: Civilian Personnel File- Destroy 1 year after separation or transfer of employee. (GRS 1-18a)

DISPOSITION NO.: C7-2

UNCLASSIFIED

**UNCLASSIFIED**

\*Correspondence File

This file contains C7 signature items, C7 notes and C7 letters.

DATE SPAN: 1990 to Present

LOCATION: C7

STORAGE MEDIA: Paper

VOLUME: 2 cu. ft.

CLASSIFICATION: TOP SECRET CODEWORD NOFORN

DISPOSITION: Documents generated by, or that are unique to,  
an organization which has program and policy  
making responsibilities.  
Permanent. Close annually. Transfer to the  
NCRC 3 years after closing. (004A-2)

DISPOSITION NO. C7-3

**UNCLASSIFIED**

**C71**  
**TRUSTED PRODUCTS**  
**AND**  
**NETWORK**  
**SECURITY**  
**EVALUATIONS**

**FOR OFFICIAL USE ONLY**

C71

Trusted Products and Network Security Evaluations

The Chief, C71, is responsible to the Chief of C7: as the source of interaction with the commercial computer industry and the execution of the Trusted Products Evaluation Program (TPEP); as the source of security evaluation support to V5, the Office of Trusted Products; as an active participant in C7 efforts regarding security criteria and standards, and the performance of security assessments; as an active participant in C7 efforts in advancement of security technologies and evaluation tools; in supporting field evaluations and research phase evaluations with information and expertise; and for maintaining the expertise and leadership needed for all of the above.

Primary functions include:

1. Performing the evaluations of the security level of computer hardware and software products that have general utility. This is accomplished in part by: developing a technical understanding of these products and determining the level of trust against the Trusted Computer Security Evaluation Criteria (TCSEC); producing the security evaluated products lists; providing guidance on trusted product development via the Vendor Assistance Program; providing feedback to computer vendors on the status and results of the evaluation on the vendors' products; providing evaluations and technical assistance on using commercially available computer security products to other members of the National Security Establishment (NSE); preparing and managing contracts for technical support of commercial product evaluations; assisting in the transfer of newly developed computer security technology to the computer industry; providing market analysis of computer product proposals to determine utility and potential in order to recommend acceptance or rejection for evaluation; determining user requirements for trusted products and heightening awareness of computer security issues.
2. Performing security evaluations of data and network systems intended to process and/or store classified information and/or unclassified, but sensitive national security related information. "Systems" include products, components, equipments, networks, and

aggregations of these items. This is accomplished in part by: developing a technical understanding of these systems, assisting with the specification of security requirements, and determining compliance to these requirements and applicable standards; identifying security deficiencies and estimating the degree of security assurance; assisting in correcting noted deficiencies; providing support to the INFOSEC Doctrine organization; providing input to endorsement, certification, and accreditation processes; providing security guidance on C71 supported programs.

3. Providing consultation and expertise to the Security Guidance Division (C75).
4. Participating in research applicable to the secure development, implementation, application, and evaluation of trusted products and secure network systems.
5. Documenting, publishing, and disseminating (as appropriate) trusted product and network system security evaluation and research results.
6. Participating in the performance of security assessments, and recommending the approval and operational use of trusted products and secure network systems based upon satisfactory security evaluation.

# UNCLASSIFIED

## Software Evaluation Manuals

This file consists of commercial software manuals and other documentation evaluated by C12 concerning computer security products.

DATE SPAN: 1983 to Present

LOCATION: C71

STORAGE MEDIA: Paper

VOLUME: 60 cu. ft.

CLASSIFICATION: UNCLASSIFIED (Proprietary Information)

DISPOSITION: Transfer to NCRC when inactive. Destroy 3 years thereafter

DISPOSITION NO. C71-1

## Evaluation File

This file contains evaluation files from private industry maintained for product evaluations.

DATE SPAN: 1985 to Present

LOCATION: C71

STORAGE MEDIA: Paper

VOLUME: 150 cu. ft.

CLASSIFICATION: UNCLASSIFIED

DISPOSITION: Destroy upon termination or completion of evaluation.

DISPOSITION NO. C71-2

UNCLASSIFIED

# UNCLASSIFIED

## ~~Product Evaluations Forum Subsystem Data Base\*~~

~~This data base consists of evaluation forums maintained for discussion, record keeping, announcement, and related purposes for product evaluations.~~

~~DATE SPAN: 1984 to Present~~

~~LOCATION: C71~~

~~STORAGE MEDIA: 3380 Disk~~

~~HARDWARE: Honeywell (DOCKMASTER)~~

~~SOFTWARE: Multics Forum Subsystem.~~

~~VOLUME: UNAVAILABLE~~

~~CLASSIFICATION: UNCLASSIFIED~~

~~DISPOSITION: Delete or destroy data when no longer needed for operations.~~

~~DISPOSITION NO.: C71-3~~

### Vendor File

This file contains listings of vendors and products.

DATE SPAN: 1987 to Present

LOCATION: C71

STORAGE MEDIA: Paper

VOLUME: 4 cu. ft.

CLASSIFICATION: UNCLASSIFIED (Proprietary Information)

DISPOSITION: Destroy when superseded or obsolete.

DISPOSITION NO.: C71-4

\*●bsolote. No longer created. See 6/12/2014 email. MPB

UNCLASSIFIED

# UNCLASSIFIED

## MITRE Support File

This file contains copies of contracts and correspondence with the Mitre Corporation.

DATE SPAN: 1982 to Present  
LOCATION: C7d  
STORAGE MEDIA: Paper  
VOLUME:  
CLASSIFICATION: SECRET  
DISPOSITION: Cut off annually. Destroy five years thereafter.  
DISPOSITION NO.: C71-5

### ~~MINSTREL File \*~~

~~This file contains documents, specifications, listings, concerning the development of electronic computer interfaces to transcribers for speech signals. Reports are sent to the Technical Library.~~

~~DATE SPAN: 1982 to Present  
LOCATION: C71  
STORAGE MEDIA: Paper  
VOLUME: 12 cu. ft.  
CLASSIFICATION: TOP SECRET CODEWORD NOFORN  
DISPOSITION: Review after certification (scheduled for 1991) Destroy when no longer needed for evaluations.  
DISPOSITION NO.: C71-6~~

\*~~Obsolete. No longer created.~~ See 6/12/2014 email  
MPB

UNCLASSIFIED

C72  
TACTICAL,  
KEY MANAGMENT,  
AND  
NATO/FOREIGN  
SYSTEMS  
EVALUATIONS

**FOR OFFICIAL USE ONLY**

C72

Tactical, Key Management, and NATO/Foreign Systems Evaluations

The Chief, C72, is responsible to the Chief of C7: as the source of security evaluation support to the following information security product development organizations: V2, V7, V8, S1, X4, and Y1; (labels may adjust pending ISSO reorganization); as an active participant in C7 efforts regarding security criteria and standards and the performance of security assessments; as an active participant in C7 efforts in advancement of security technologies and evaluation tools; in supporting field evaluations and research phase evaluations with information and expertise; and for maintaining expertise and leadership needed for all of the above.

Primary functions include:

1.



NSA25X6

- a. developing a technical understanding of these systems, assisting with the identification of security requirements, and determining compliance to these requirements and applicable standards;
  - b. identifying security deficiencies, and estimating the degree of security assurance;
  - c. assisting in correcting noted deficiencies;
  - d. providing support to the INFOSEC Doctrine Organization;
  - e. providing input to endorsement, certification and accreditation processes;
  - f. providing security guidance on C72 supported programs.
2. Providing consultation and expertise to the Security Guidance Division (C75).

3. Participating in research applicable to the secure development, implementation, application, and evaluation of Tactical, Key Management, [ e ] and products developed through the INFOSEC Design & Manufacturing Center.
4. Documenting, publishing, and disseminating (as appropriate) system security evaluations and research results.
5. Participating in the performance of security assessments, and recommending the approval and operational use of Tactical, Key Management, [ ] and products developed through the INFOSEC & Manufacturing Center, based upon satisfactory security evaluation.
6. Establishing and maintaining technical liaison with all appropriate organizations both internal and external to ISSO/NSA.

# UNCLASSIFIED

## Research and Analysis File

This file includes records documenting research and analysis efforts in evaluation, assessment, and math techniques. Included are records documenting program management.

DATE SPAN: 1960 to Present

LOCATION: C72

STORAGE MEDIA: Paper

VOLUME: 40 cu. ft.

CLASSIFICATION: TOP SECRET CODEWORD NOFORN

DISPOSITION: Permanent. Transfer to NCRC when no longer needed for operations.

DISPOSITION NO.: C72-1

UNCLASSIFIED

**UNCLASSIFIED**

COMSEC Equipment File

This file consists of correspondence and technical reports pertaining to equipment descriptions, proposed equipment, modifications, procedural modifications of doctrine, and specifications.

DATE SPAN: 1978 to Present

LOCATION: C7E

STORAGE MEDIA: Paper

VOLUME: 6 cu. ft.

CLASSIFICATION: TOP SECRET

DISPOSITION: Permanent. Transfer to NCRC when no longer needed for operations.

DISPOSITION NO. : C7E-2

**UNCLASSIFIED**

UNCLASSIFIED

~~ADPS Reports Control Case Folders~~ \*

~~This file consists of correspondence between consumers and NSA management. The correspondence relates to report requests, report formats, number of copies, distribution, classification, and any other information pertaining to automated data processing systems case files.~~

~~DATE SPAN: 1978 to Present~~

~~LOCATION: C7E~~

~~STORAGE MEDIA: Paper~~

~~VOLUME: .3 cu. ft.~~

~~CLASSIFICATION: SECRET NOFORN~~

~~DISPOSITION: Destroy when no longer needed for operations~~

~~DISPOSITION NO.: C72-3~~

\*C72 Personnel Files

This file consists of folders for each member of the division and contain copies of personnel summaries, performance appraisals and other similar forms.

DATE SPAN: indefinite

LOCATION: C7E

STORAGE MEDIA: Paper

VOLUME: 1 cu. ft.

CLASSIFICATION: TOP SECRET CODEWORD NOFORN

DISPOSITION: Civilian Personnel File- Destroy 1 year after separation or transfer of employee. (GRS 1-18a)

DISPOSITION NO.: C72-4

\*~~Obsolete. No longer created. See 6/12/2014 email. MPB~~

# UNCLASSIFIED

## \*Chronological Correspondence Files

This file contains copies of correspondence originated by C72.

DATE SPAN: July 1990 to Present  
LOCATION: C72  
STORAGE MEDIA: Paper  
VOLUME: .25 cu. ft.  
CLASSIFICATION: CODEWORD NOFORN  
DISPOSITION: Destroy when 3 years old or sooner if no longer required for operations. (GRS 23-1)  
DISPOSITION NO.: C72-5

## \*Administrative Communications Files

This file consists of copies of travel requests. It also consists of copies of clearance and special access requests for members of C72.

DATE SPAN: July 1990 to Present  
LOCATION: C72  
STORAGE MEDIA: Paper  
VOLUME: .2 cu. ft.  
CLASSIFICATION: SECRET  
DISPOSITION: Destroy when 3 years old or sooner if no longer required for operations. (GRS 23-1)  
DISPOSITION NO.: C72-6

UNCLASSIFIED

# UNCLASSIFIED

## \*C721 Personnel Files

This file consists of personnel files for branch members.

DATE SPAN: 1989 to Present

LOCATION: C721

STORAGE MEDIA: Paper

VOLUME: .5 cu. ft.

CLASSIFICATION: TOP SECRET CODEWORD NOFORN

DISPOSITION: Civilian Personnel File- Destroy 1 year after separation or transfer of employee. (GRS 1-18a)

DISPOSITION NO: C72-7

UNCLASSIFIED

UNCLASSIFIED

\*C722 Personnel Files

This file contains personnel records for individuals in C722.

DATE SPAN: 1989 to Present  
LOCATION: C722  
STORAGE MEDIA: Paper  
VOLUME: .75 cu. ft.  
CLASSIFICATION: TOP SECRET  
DISPOSITION: Civilian Personnel File- Destroy 1 year after separation or transfer of employee. (GRS 1-18a)  
DISPOSITION NO.: C72-8

~~\*Project Information Files \*~~

~~This file consists of information on all projects being evaluated for key management: EKMS, DTO, KMD/KP, SDNS KMS, NKDS, LRIP DTO, SKMM, FIRRS, Central Facility II and CIA projects: Cherrystem and Crane. Also NGS II.~~

~~DATE SPAN: 1986 to Present  
LOCATION: C722  
STORAGE MEDIA: Paper  
VOLUME: 65.25 cu. ft.  
CLASSIFICATION: TOP SECRET CODEWORD  
DISPOSITION: A. OPI- Permanent. Close annually and transfer to the NCRC when no longer required for operations.  
B. All others- Destroy when program is completed, cancelled or becomes obsolete. (002)  
DISPOSITION NO.: C72-9 A and B~~

\*●bsolte. No longer created. See 6/12/2014 email. MPB

UNCLASSIFIED

**UNCLASSIFIED**

\*C723 Personnel Files

This file consists of personnel records for C723.

DATE SPAN:

LOCATION: C723

STORAGE MEDIA: Paper

VOLUME: 2 cu. ft.

CLASSIFICATION: TOP SECRET CODEWORD NOFORN

DISPOSITION: Civilian Personnel File- Destroy 1 year after separation or transfer of employee. (GRS 1-18a)

DISPOSITION NO.: C72-10

**DELETED: 18 NOV. 1991**

~~Cryptogeneration File~~ \*

~~This file contains documents and listings of documents used in support of COMPUSEC activities taken from previous evaluations. This is essentially used as a reference file.~~

~~DATE SPAN: 1971 to Present~~

~~LOCATION: C72~~

~~STORAGE MEDIA: Paper~~

~~VOLUME: 20 cu. ft.~~

~~CLASSIFICATION: TOP SECRET CODEWORD NOFORN~~

~~DISPOSITION: Destroy when no longer needed for operations.~~

~~DISPOSITION NO.: C72-11~~

\*Obsolete. No longer created. See 6/12/2014 email. MPB

**UNCLASSIFIED**

**C73**  
**SPACE, WEAPONS,**  
**TRANSEC SIGNALS**  
**AND**  
**STRATEGIC SYSTEMS**  
**SECURITY**  
**EVALUATIONS**

**FOR OFFICIAL USE ONLY**

C73

Space, Weapons, TRANSEC/Signals and Strategic Systems  
Security Evaluations

The Chief, C73, is responsible to the Chief of C7: as the source of security evaluation support to the following information security product development organizations: V4, V6,...(to be determined after ISSO reorganization); as an active participant in C7 efforts regarding security criteria and standards and the performance of security assessments; as an active participant in C7 efforts in advancement of security technologies and evaluation tools; in supporting field evaluations and research phase evaluations with information and expertise; and for maintaining the expertise and leadership needed for all of the above.

Primary functions include:

1. Performing security evaluations of space, weapons, TRANSEC/signals, and strategic systems. "Systems" include product components, equipments, networks, and aggregations of these. This is accomplished, in part, by:
  - a. developing a technical understanding of these systems, assisting with the identification of security requirements, and determining compliance to these requirements and applicable standards;
  - b. identifying security deficiencies, and estimating the degree of security assurance;
  - c. assisting in correcting noted deficiencies;
  - d. providing support to the INFOSEC Doctrine Organization;
  - e. providing input to endorsement, certification and accreditation processes;
  - f. providing security guidance on C73 supported programs.
2. Providing consultation and expertise to the Security Guidance Division (C75).
3. Participating in research applicable to the secure development, implementation, application, and evaluation

~~CONFIDENTIAL~~

relating to space, weapons, TRANSEC/signals, and strategic systems.

4. Documenting, publishing, and disseminating (as appropriate) INFOSEC evaluations and research results.
5. Participating in the performance of security assessments, and recommending the approval and operational use of space, weapons, and strategic systems, based upon satisfactory security evaluation.
6. Establishing and maintaining technical liaison with all appropriate organizations both internal and external to ISSO/NSA.

~~CONFIDENTIAL~~

**UNCLASSIFIED**

Secure Communications Systems File

This file includes data on the evaluation of the overall security effectiveness of DoD communications systems, weapons systems, and specialized defense systems.

DATE SPAN: 1948 to Present  
LOCATION: C73  
STORAGE MEDIA: Paper  
VOLUME: 30 cu. ft.  
CLASSIFICATION: TOP SECRET NOFORN  
DISPOSITION: Permanent. Transfer to NCRC when no longer needed for operations.  
DISPOSITION NO.: C73-1  
DELETED: 22 NOVEMBER 1991

103-13

**UNCLASSIFIED**

Evaluation Documentation File

This file contains NSA evaluation papers concerning logic, equipment, and systems security for space, Command, Control, and Communications (C3), voice and data systems applications.

DATE SPAN: 1975 to Present  
LOCATION: C73  
STORAGE MEDIA: Paper  
VOLUME: 30 cu. ft.  
CLASSIFICATION: TOP SECRET NOFORN  
DISPOSITION: Permanent. Transfer to NCRC when no longer needed for operations.  
DISPOSITION NO.: C73-2  
**DELETED** 22 NOVEMBER 1991

103-14

COMSEC Analysis Reports File

This file contains analytical studies of U.S. and allied communications.

DATE SPAN: 1970 to Present  
LOCATION: C73  
STORAGE MEDIA: Paper  
VOLUME: 45 cu. ft.  
CLASSIFICATION: TOP SECRET CODEWORD NOFORN  
DISPOSITION: Permanent. Transfer to NCRC when no longer needed for operations.  
DISPOSITION NO.: C73-3  
**DELETED** 22 NOVEMBER 1991

103-15

**FOR OFFICIAL USE ONLY**

**UNCLASSIFIED**

Engineer's Equipment Project/Case File

This file contains data generated during the development, production, and operational phases of equipment.

DATE SPAN: 1976 to Present  
LOCATION: C73  
STORAGE MEDIA: Paper  
VOLUME: 12 cu. ft.  
CLASSIFICATION: TOP SECRET CODEWORD  
DISPOSITION: Permanent. Transfer to NCRC when no longer needed for operations.  
DISPOSITION NUMBER: C73-4  
**DELETED** 22 NOVEMBER 1991

103-16

**UNCLASSIFIED**

**UNCLASSIFIED**

Correspondence File

This file contains incoming and outgoing letters, memoranda, reports and other records reflecting computer security evaluation.

DATE SPAN: 1981 to Present

LOCATION: C73

STORAGE MEDIA: Paper

VOLUME: .2 cu. ft.

CLASSIFICATION: TOP SECRET CODEWORD NOFORN

DISPOSITION: Close annually Destroy after 3 years or sooner if no longer required for operations. (GRS 23-1)

DISPOSITION NO.: C73-5

Suspense Log Data Base

DISPOSITION NO. C73-6

**TRANSFERRED TO: C91-6 20 NOV. 1991**

**UNCLASSIFIED**

# UNCLASSIFIED

## Travel Data Base

This data base contains information on the travel activities of C7 employees.

DATE SPAN: 1986 to Present

LOCATION: C73

STORAGE MEDIA: Magnetic disk

HARDWARE: PC

SOFTWARE: DB III

VOLUME: 1 floppy disk

CLASSIFICATION: UNCLASSIFIED

DISPOSITION: Destroy when 3 years old or sooner if no longer required for operations. (GRS 23-1)

DISPOSITION NO: C73-7

**DELETED: 22 NOVEMBER 1991**

### \*Personnel File

This file contains personnel folders for each person in C73.

DATE SPAN:

LOCATION: C73

STORAGE MEDIA: Paper

VOLUME: 2 cu ft.

CLASSIFICATION: TOP SECRET CODEWORD

DISPOSITION: Civilian Personnel File- Destroy 1 year after separation or transfer of employee (GRS 1-18a)

DISPOSITION NO.: C73-8

UNCLASSIFIED

**UNCLASSIFIED**

**C74**  
**IMPLEMENTATIONS**  
**SECURITY**

**UNCLASSIFIED**

C74

Implementations Security

The Chief, C74, is responsible to the Chief of C7: as the source of CV (Cryptographic Verification), SFA (Security Fault Analysis), and TECHSEC (Technical Security) evaluations; as a major participant in C7 efforts in advancement of CV, SFA, and TECHSEC technologies and tools; in supporting CV, SFA, and TECHSEC sections of fielded evaluations, research phase evaluations, and standards with information and expertise; and for maintaining the expertise and leadership needed for all of the above.

NSA25X6

Primary functions include:

1.



2. Participation in CV, SFA, and TECHSEC research applicable to the secure development, implementation, application and evaluation of systems.
3. Supporting the TEMPEST Professional Certification Program and the Tempest Endorsement Program.
4. Documenting, publishing and disseminating (as appropriate) CV, SFA, TECHSEC evaluations and research results.
5. Providing justification for the CV, SFA, and TECHSEC program budget items, and supporting C7 in preparing those items.
6. Establishing and maintaining technical liaison with all appropriate CV, SFA, and TECHSEC organizations both internal and external to NSA/ISSO.
7. Assisting the Chief, C, in providing NSA leadership and representation in various technical security forums.

**UNCLASSIFIED**

Daily Correspondence File

This file contains copies of all correspondence arranged in chronological order.

DATE SPAN: Oct.1990 to Present  
LOCATION: C74  
STORAGE MEDIA: Paper  
VOLUME: 1 cu. ft.  
CLASSIFICATION: TOP SECRET CODEWORD NOFORN  
DISPOSITION: Close annually. Destroy after 3 years or sooner if no longer required for operations. (GRS 23-1)  
DISPOSITION NO.: C74-1

~~25-5 Projects File \*~~

~~This file is the "historical record" of the COMPUSEC procurement responses to Program Budget System (PBS) I and III, and Systems Acquisition Plans (SAPs).~~

~~DATE SPAN: 1980 to Present  
LOCATION: C74  
STORAGE MEDIA: Paper  
VOLUME: 30 cu. ft.  
CLASSIFICATION: TOP SECRET CODEWORD NOFORN  
DISPOSITION: Permanent. Transfer to the NCRC at the end of the program cycle or when no longer required for reference purposes. (002D 1a)  
DISPOSITION NO.: C74-2  
DELETED: 18 NOV. 1991~~

\***●**obsolete. No longer created. See 6/12/2014 email  
**MPB**

**UNCLASSIFIED**

MINSTREL File

DISPOSITION NO.n C74-3

**TRANSFERRED TO** C71-6 21 OCT. 1991

T Operating System (TOS) File

DISPOSITION NO.n C74-4

**TRANSFERRED TO** C91-5 21 OCT. 1991

**UNCLASSIFIED**

UNCLASSIFIED

OVERTAKE File \*

This file contains documents, specifications, and listings concerning the design and development of standardized COMSEC products to secure classified and unclassified traffic. Reports are sent to the Technical Librarye

~~DATE SPAN:~~ 1985 to Present

~~LOCATION:~~ C74

~~STORAGE MEDIA:~~ Paper

~~VOLUME:~~ 4 cu. ft.

~~CLASSIFICATION:~~ SECRET

~~DISPOSITION:~~ Destroy after two years or when no longer needed for operations, whichever is later.

~~DISPOSITION NO.:~~ C74-5

~~DELETED:~~ 26 NOVEMBER 1991

~~Cryptogeneration File~~

~~DISPOSITION NO.:~~ C74-6

~~TRANSFERRED TO:~~ C72-11 21 OCT. 1991

\*Obsolete. No longer created. See 6/12/2014 email  
MPB

C74-5  
Overtake File  
(C62-transfer?)

UNCLASSIFIED

# UNCLASSIFIED

## \*SFA/TEMPEST/CV File

This file contains Security Fault Analysis, Tempest, and Cryptologic Verification information concerning the impact of potential system security failures and confirmation of implemented designs.

DATE SPAN: Oct 1990-Present  
LOCATION: C74  
STORAGE MEDIA: Paper  
VOLUME: 15 cu. ft.  
CLASSIFICATION: TOP SECRET CODEWORD NOFORN  
DISPOSITION: Retained locally. Destroy when no longer needed for operations.  
DISPOSITION NO.: C74-7

## \*Implementation Evaluation Reports and Technical Notes File

This file contains reports and notes concerning the implementation of systems.

DATE SPAN: Oct 1990-Present  
LOCATION: C74  
STORAGE MEDIA: Paper  
VOLUME: 3 cu. ft.  
CLASSIFICATION: TOP SECRET CODEWORD NOFORN LACONIC NOCONTRACT  
DISPOSITION: Close annually. Transfer to the NCRC. Destroy after 5 years or sooner if no longer required for operations.  
DISPOSITION NO.: C74-8

UNCLASSIFIED

# UNCLASSIFIED

~~\*PDB TOOL File \*~~

~~This file is a Project Data Base of evaluations and status reports, timelines, and equipment problems.~~

~~DATE SPAN: Oct 1990-Present~~

~~LOCATION: C74~~

~~STORAGE MEDIA: Disk~~

~~HARDWARE: SUN~~

~~SOFTWARE:~~

~~VOLUME:~~

~~CLASSIFICATION: TOP SECRET CODEWORD NOFORN LACONIC NOCONTRACT~~

~~DISPOSITION: Close annually. Delete or destroy when no longer required for operations.~~

~~DISPOSITION NO.: C74-9~~

\*Weekly Items File

This file consists of the read file.

DATE SPAN: Oct 1990-Present

LOCATION: C74

STORAGE MEDIA: Disk/Floppy

HARDWARE: SUN/PC

SOFTWARE:

VOLUME:

CLASSIFICATION: TOP SECRET CODEWORD NOFORN

DISPOSITION: Close annually. Delete or destroy when no longer required for operations.

DISPOSITION NO.: C74-10

\*~~Ob~~solete. No longer created. See 6/12/2014 email. MPB

# UNCLASSIFIED

# UNCLASSIFIED

## \*Monthly Activity Report File

This file contains the monthly activity reports for C74.

DATE SPAN: Oct 1990-Present  
LOCATION: C74  
STORAGE MEDIA: Paper  
VOLUME: 1 cu. ft.  
CLASSIFICATION: TOP SECRET CODEWORD NOFORN  
DISPOSITION: Close annually. Destroy after 3 years or sooner if no longer required for operations.  
DISPOSITION NO.: C74-14

## \*Clearance File

This file contains information for security on clearances for contractors.

DATE SPAN: Oct 1990-Present  
LOCATION: C74  
STORAGE MEDIA: Paper  
VOLUME: 1 cu. ft.  
CLASSIFICATION: TOP SECRET CODEWORD  
DISPOSITION: Close annually. Destroy when superseded or updated.  
DISPOSITION NO.: C74-12

UNCLASSIFIED

**UNCLASSIFIED**

**C75**  
**SECURITY**  
**GUIDANCE**

**UNCLASSIFIED**

C75

Security Guidance

The Chief, C75, is responsible to the Chief of C7: as the source of security guidance support to information security product development organizations and the Systems Engineering Organizations (S9); for developing and implementing an orderly and efficient process by which information systems may be developed securely with maximum assurance; and for maintaining the expertise and leadership needed for the above.

Primary functions include:

1. Providing scientific security expertise and guidance during the development of systems supported by C7.
2. Developing and implementing an orderly and efficient process by which information systems may be securely deployed with maximum assurance.
3. Conducting and/or attending security architecture reviews to assist system developers in the design of appropriately secured systems.
4. Developing requirements for automated tools and expert systems to expedite and facilitate the development of secure systems.
5. Assisting C71, C72, C73 in providing Functional Security Requirements Specifications (FSRS) for programs supported in those divisions; and providing tailored FSRS for all other programs.
6. Resolving conflicts between system and security requirements and providing guidance and/or assistance in correcting noted deficiencies.
7. Identifying system and cryptanalytic problems requiring comprehensive security evaluation.
8. Maintaining a log or audit trail of security-related decisions and trade-offs between system and security requirements.

# UNCLASSIFIED

## Cryptosecurity Assessment File

This file includes evaluation and analysis records generated by NSA analysts regarding cryptosecurity assessment.

DATE SPAN: 1982 to Present  
LOCATION: C75  
STORAGE MEDIA: Paper  
VOLUME: 20 cu. ft.  
CLASSIFICATION: TOP SECRET NOFORN  
DISPOSITION: Permanent. Transfer to NCRC when no longer needed for operations.  
DISPOSITION NO.: C75-1

## \*Administrative Communications File

This file contains copies of C75 centralized travel requests, copies of transmittals, National Cryptologic School Bulletins, notes for C Staff meetings, reports of award recipients, course nominations and training requirements, and memorandum.

DATE SPAN: Aug. 1990 to Present  
LOCATION: C75  
STORAGE MEDIA: Paper  
VOLUME: cu. ft.  
CLASSIFICATION: TOP SECRET CODEWORD NOFORN  
DISPOSITION: Destroy when 3 years old or when no longer required for operations. (GRS 23-1)  
DISPOSITION NO.: C75-2

UNCLASSIFIED

**UNCLASSIFIED**

\*Personnel Information File

This file contains personnel information on individuals in C75n

DATE SPAN: Aug. 1990 to Present

LOCATION: C75

STORAGE MEDIA: Paper

VOLUME: cu. ft.

CLASSIFICATION: UNCLASSIFIED

DISPOSITION: Civilian Personnel File- Destroy 1 year after  
separation or transfer of employee.  
(GRS 1-18a)

DISPOSITION NO.: C75-3

**UNCLASSIFIED**

# UNCLASSIFIED

## \*C75 Memoranda File

This file contains all correspondence that C75 has written: memorandums, M/R, and letters.

DATE SPAN: Aug. 1990 to Present  
LOCATION: C75  
STORAGE MEDIA: Paper  
VOLUME: cu. ft.  
CLASSIFICATION: TOP SECRET CODEWORD NOFORN  
DISPOSITION: Close annually. Destroy after 3 years or sooner if no longer required for operations. (GRS 23-1)  
DISPOSITION NO. n C75-4

## \*Weekly Items of Interest File

This file contains C6, C7, C8, and C9 weekly items of interest.

DATE SPAN: Aug. 1990 to Present  
LOCATION: C75  
STORAGE MEDIA: Paper  
VOLUME: cu. ft.  
CLASSIFICATION: TOP SECRET CODEWORD NOFORN  
DISPOSITION: Delete or destroy after 2 years.  
DISPOSITION NO. n C75-5

UNCLASSIFIED

# UNCLASSIFIED

## \*Information File

This file contains organizational phone lists and charts and information on rules and regulations.

DATE SPAN: Aug. 1990 to Present  
LOCATION: C75  
STORAGE MEDIA: Paper  
VOLUME: cu. ft.  
CLASSIFICATION: TOP SECRET CODEWORD NOFORN  
DISPOSITION: Delete or destroy after 3 years or sooner if no longer required for operations. (GRS 23-1)  
DISPOSITION NO.: C75-6

## \*C Technical Literature Award File

This file contains memorandums about the C Technical Literature Award.

DATE SPAN: Aug. 1990 to Present  
LOCATION: C75  
STORAGE MEDIA: Paper  
VOLUME: cu. ft.  
CLASSIFICATION: UNCLASSIFIED  
DISPOSITION: Destroy 2 years after approval or disapproval. (GRS 1-12)  
DISPOSITION NO.: C75-7

UNCLASSIFIED

**UNCLASSIFIED**

\*Clearances File

This file contains clearance certification requests.

DATE SPAN: Aug. 1990 to Present

LOCATION: C75

STORAGE MEDIA: Paper

VOLUME: cu. ft.

CLASSIFICATION: UNCLASSIFIED

DISPOSITION: Destroy 2 years after authorization expires.  
(GRS 18-6)

DISPOSITION NO.: C75-8

**UNCLASSIFIED**

# UNCLASSIFIED

\*Business Developmental Council File

This file contains M/R (memorandums for the record) dealing with Business Development Council meetings.

DATE SPAN: Aug. 1990 to Present

LOCATION: C75

STORAGE MEDIA: Paper

VOLUME:

CLASSIFICATION: TOP SECRET CODEWORD VRK NOFORN

DISPOSITION: Close annually. Destroy after 3 years or sooner if no longer required for operations.  
(GRS 23-1)

DISPOSITION NO. C75-9

UNCLASSIFIED

**UNCLASSIFIED**

**C76**

**ADVANCED TECHNOLOGY**

**AND**

**FUTURE SYSTEM**

**SECURITY**

**GUIDANCE**

**UNCLASSIFIED**

## Advanced Technology and Future System Security Guidance

The Chief of C76 is responsible to the Chief of C7: as the source of security guidance for information security products which contain advanced techniques or utilize futuristic technology which lacks the history upon which most security guidance is based; for the support of customers which include all development organizations of such products; as the source of security guidance for advanced techniques used by the Office of Key Management (V8); and for maintaining the expertise and leadership needed for the above.

Primary functions include:

1. Development/discovery of the underlying scientific principles upon which security guidance should be based.
2. Generation of guidance for use by developers which is based on scientific principles and analysis.
3. Promotion of advanced techniques which will improve the security of future ISSO products.
4. Development/discovery of synergistic techniques which will improve the security of future ISSO products.
5. Aiding development organizations in dealing with security relevant aspects of design.
6. Providing development organizations with both generic and specialized development aids (keying material, test material, etc.).
7. Participating in research applicable to advanced technology and future ISSO systems.

# UNCLASSIFIED

## \*Administrative File

This file contains copies of clearances, special access requests, NCS courses, NCS bulletins, course withdrawals, external training, travel requests, transmittals, and PR's.

DATE SPAN: Jan 1989 to Present  
LOCATION: C76  
STORAGE MEDIA: Paper  
VOLUME: 2 cu. ft.  
CLASSIFICATION: TOP SECRET NOFORN  
DISPOSITION: Close annually. Destroy after 3 years or sooner if no longer required for operations. (GRS 23-1)  
DISPOSITION NO.: C76-1

## \*Personnel File

This file contains personnel information on each C76 individual.

DATE SPAN: 1989 to Present  
LOCATION: C76  
STORAGE MEDIA: Paper  
VOLUME: 1 cu. ft.  
CLASSIFICATION: TOP SECRET NOFORN  
DISPOSITION: Destroy 1 year after transfer or separation of employee. (GRS 1-18a)  
DISPOSITION NO.: C76-2

UNCLASSIFIED

UNCLASSIFIED

\*Correspondence File

This file contains copies of correspondence originated by C76.

DATE SPAN: July 1987 to Present  
LOCATION: C76  
STORAGE MEDIA: Paper  
VOLUME: 1 cu. ft.  
CLASSIFICATION: TOP SECRET NOFORN  
DISPOSITION: Destroy when 3 years old or sooner if no longer needed for operations. (GRS 23-1)  
DISPOSITION NO. n C76-3

~~\*Technical Library File \*~~

~~This file consists of a collection of manuals and memos.~~

~~DATE SPAN: Feb 1959 to Present  
LOCATION: C76  
STORAGE MEDIA: Paper  
VOLUME: 100 cu. ft.  
CLASSIFICATION: TOP SECRET NOFORN  
DISPOSITION: A. OPI Produced or Unique Materials - Permanent. Relocate to the NCRC when no longer required for operations.  
B. All others - Destroy when no longer required for operations. (002B)  
DISPOSITION NO. s C76-4 A and B~~

\*●obsolete. No longer created. See 6/12/2014 email. MPB

UNCLASSIFIED

# UNCLASSIFIED

## Key Management Reference Material File

This file consists of background and reference information pertaining to key management and COMSEC equipment design.

DATE SPAN: 1965 to Present

LOCATION: C76

STORAGE MEDIA: Paper/Floppy Disks

HARDWARE: KIWI -VAX 8600

SOFTWARE: KIWI -VMS OPERATING SYSTEM

VOLUME: 47 cu. ft.

CLASSIFICATION: TOP SECRET CODEWORD, NOFORN, VRK

DISPOSITION: A. Hard Copy: Permanent. Retire to NSA Archives.

B. Electronic Copy: Destroy when no longer needed for reference purposes.

DISPOSITION NO.n C76-5 A and B

PREVIOUSLY V81-1 A and B 920309

UNCLASSIFIED

**C8**  
**INFOSEC**  
**STANDARDS,**  
**ASSESSMENTS,**  
**AND**  
**SYSTEM SERVICES**

**FOR OFFICIAL USE ONLY**

C8

INFOSEC Standards, Assessments, and System Services

The Chief, C8, is responsible to the Chief, C, for developing and maintaining technical standards and criteria to foster the production and evaluation of quality INFOSEC products and services; performing security risk assessments and developing risk methodologies, threat models and vulnerability databases; developing, operating and maintaining computer systems, services, networks and tools to support elements within C and the ISSO; and supporting C security evaluation efforts.

Primary functions include:

1. Developing , coordinating, publishing and maintaining INFOSEC standards, criteria and guidelines to foster the production and evaluation of quality INFOSEC products and services aimed at a broad range of customers. Specific examples include the "Rainbow Series" of computer security publications, an INFOSEC Criteria (Gold Book) that synthesizes the Functional Security Requirements Specification (FSRS) and the Trusted Computer Systems Evaluation Criteria (TCSEC), cryptographic standards, related costing manuals, and technical security standards.
2. Performing risk assessments on INFOSEC programs and products to support management decisions on acceptability of INFOSEC products.
3. Researching, developing, and implementing threat models and vulnerability databases in support of risk assessments, evaluations, and other functions.
4. Investigating new methodologies for performing security assessments, costing, and other missions within C8.
5. Supporting C security evaluation efforts and participating in research and development in direct support of the C mission.
6. Developing, operating, and maintaining computer systems, services, networks and tools to perform the primary functions in paragraphs 1 to 5 above. This function includes operating the current DOCKMASTER System and managing the DOCKMASTER II acquisition.

**FOR OFFICIAL USE ONLY**

**UNCLASSIFIED**

Administrative File

This file includes all correspondence generated and received by C8 dealing with travel, training, security, personnel, and related matters.

DATE SPAN: 1986 to Present

LOCATION: C8

STORAGE MEDIA: Paper

VOLUME: 20 cu. ft.

CLASSIFICATION: SECRET

DISPOSITION: A. Personnel file- Destroy 1 year after transfer or separation of employee (GRS 1-18a) (003-1)

B. All others- Destroy when 3 years old or when no longer required for operations (GRS 23-1) (001B)

DISPOSITION NO.: C8-1 A and B

**UNCLASSIFIED**

**UNCLASSIFIED**

**C81  
STANDARDS,  
CRITERIA,  
AND  
GUIDELINES**

**UNCLASSIFIED**

## Standards, Criteria and Guidelines

The Chief of Standards, Criteria and Guidelines Division is responsible to the Chief of the Office of INFOSEC Standards, Assessments, and Systems Services for developing and maintaining technical Information Systems Security (INFOSEC) criteria, interpretations, and guidelines for use within the Department of Defense and Intelligence Community.

Primary functions include:

1. Managing the development of cryptographic standards, technical security standards, and computer security standards, and guidelines under the auspice of the INFOSEC Technical Guidelines Program.
2. Supporting the INFOSEC Evaluation Programs through the development and publication of INFOSEC technical guidelines in accordance with Trusted Computer System Evaluation Criteria (TCSEC) and the Functional Security Requirements Specifications (FSRS) for evaluators, vendors, developers and users of trusted INFOSEC products.
3. Developing and maintaining expertise in technical INFOSEC issues to promote the advancement of security evaluation tools and trust technology.
4. Creating an INFOSEC criteria that clearly delineates linkages between "type" vs "level-of-trust." This implies an integration of the FSRS and TCSEC documents.
5. Supporting field evaluations, developmental evaluations, and research phase evaluations with standards, criteria, assessments, and expertise.
6. Developing and maintaining profiles needed to identify the relationship between TCSEC levels-of-trust and specific threats.
7. Maintaining an open dialogue with commercial and technical communities regarding Computer Security (COMPUSEC) criteria and interpretations. Serve as the NSA single point of contact for the development of international COMPUSEC criteria.

8. Increasing systems security understanding through recommendations on how to operate ADP systems securely in specific environments.
9. Providing technical input to the development or revision of Department of Defense, Intelligence Community and Federal INFOSEC policies, directives and instructions. Providing technical and administrative support to INFOSEC committees and subcommittees.

**FOR OFFICIAL USE ONLY**

# UNCLASSIFIED

## TNI Comments Data Base

This data base is a forum for cataloging comments on the Trusted Network Interpretations Documents

DATE SPAN: Under Development  
LOCATION: C81  
STORAGE MEDIA: Hard Disk  
HARDWARE: DOCKMASTER  
VOLUME: UNAVAILABLE  
CLASSIFICATION: UNCLASSIFIED  
DISPOSITION: Delete data when 2 years old.  
DISPOSITION NO.: C81-1

## ~~DBMS Guideline Forum Data Base \*~~

~~This data base is a forum for discussions concerning Trusted Data Base Management Systems.~~

~~DATE SPAN: Under Development  
LOCATION: C81  
STORAGE MEDIA: Hard Disk  
HARDWARE: DOCKMASTER  
VOLUME: UNAVAILABLE  
CLASSIFICATION: UNCLASSIFIED  
DISPOSITION: Delete data when 2 years old.  
DISPOSITION NO.: C81-2~~

\*~~Obsolete. No longer created. See 6/12/2014 email. MPB~~

UNCLASSIFIED

# UNCLASSIFIED

## ~~Trusted UNIX Data Base\*~~

~~This data base is a forum to catalog ideas, minutes, and agenda items for the Trusted UNIX Project.~~

~~DATE SPAN: Under Development~~  
~~LOCATION: C81~~  
~~STORAGE MEDIA: Hard Disk~~  
~~HARDWARE: DOCKMASTER~~  
~~VOLUME: UNAVAILABLE~~  
~~CLASSIFICATION: UNCLASSIFIED~~  
~~DISPOSITION: Delete data when 2 years old.~~  
~~DISPOSITION NO.n C81-3~~

## ~~TNI Discussion Data Base \*~~

~~This data base is a forum for Trusted Network Interpretation Discussions.~~

~~DATE SPAN: Under Development~~  
~~LOCATION: C81~~  
~~STORAGE MEDIA: Hard Disk~~  
~~HARDWARE: DOCKMASTER~~  
~~VOLUME: UNAVAILABLE~~  
~~CLASSIFICATION: UNCLASSIFIED~~  
~~DISPOSITION: Delete data when 2 years old.~~  
~~DISPOSITION NO.n C81-4~~

\*~~Obsolete. No longer created.~~ See 6/12/2014 email. MPB

UNCLASSIFIED

# UNCLASSIFIED

## ~~TNI Interpretations Data Base~~ \*

~~This data base is a forum for cataloging interpretations for networks derived from the "Trusted Computer System Evaluation Criteria."~~

~~DATA SPAN: Under Development~~  
~~LOCATION: C81~~  
~~STORAGE MEDIA: Hard Disk~~  
~~HARDWARE: DOCKMASTER~~  
~~VOLUME: UNAVAILABLE~~  
~~CLASSIFICATION: UNCLASSIFIED~~  
~~DISPOSITION: Delete data when 2 years old~~  
~~DISPOSITION NO.: C81-5~~

## TNG Data Base

This data base contains a master copy of the Trusted Network Guide-line.

DATE SPAN: Under Development  
LOCATION: C81  
STORAGE MEDIA: Hard Disk  
HARDWARE: DOCKMASTER  
VOLUME: UNAVAILABLE  
CLASSIFICATION: UNCLASSIFIED  
DISPOSITION: Master Data Base- Delete after retention period of hard copy media or when no longer needed for operations. (004C-1) (GRS 20-3)  
DISPOSITION NO.: C81-6

\*~~o~~bsol~~e~~. No longer created. See 6/12/2014 email. MPB

UNCLASSIFIED

**UNCLASSIFIED**

**C82**  
**RISK ASSESSMENT**  
**AND**  
**THREAT MODELS**

**UNCLASSIFIED**

## Risk Assessment and Threat Models

The Chief of the Risk Assessment and Threat Models Division is responsible to the Chief of the Office of INFOSEC Standards, Assessments, and System Services for the assessment of risk to exploitation of U.S. INFOSEC equipments and systems, and their applications; and for the establishment of threat models. The threat models must as accurately as possible reflect the current and future threat to U.S. INFOSEC equipments, systems, and techniques presented by other countries or organizations. The output of the risk assessment process is intended to be an aid to corporate level INFOSEC management who must determine which vulnerabilities and problems have to be countered and which can be considered "accepted risks."

Primary functions include:

1. Creating and maintaining models, which as accurately as possible reflect the current and future threat to the U.S. by other countries or organizations, in the following threat areas:
  - a. U.S. and NATO classified information which is or will be protected by U.S. Government INFOSEC equipments, systems, or techniques;
  - b. U.S. unclassified national security-related information which is or will be protected by U.S. Government INFOSEC equipments, systems or techniques;
  - c. U.S. facilities which will or do use U.S. Government INFOSEC equipments, systems or techniques; and
  - d. National security-related actions, such as unauthorized missile launch, which are or will be protected by U.S. Government INFOSEC equipments, systems or techniques.
2. Levying requirements and tasking on ISSO's threat analysis organization for the purpose of obtaining support for developing threat models.
3. Developing and maintaining a methodology for a risk assessment process for the U.S. Government INFOSEC

**FOR OFFICIAL USE ONLY**

equipments and systems which takes into account the threat model, known vulnerabilities, security evaluation standards, countermeasures, confidence and application specific considerations

4. Developing and maintaining a methodology for a risk assessment process for the U.S. Government INFOSEC equipments, systems or techniques which takes into account the application specific threat model, known residual INFOSEC equipment and system vulnerabilities, site countermeasures and application specific considerations such as the occurrence of unusual events.
5. Tasking internal and external organizations for data on a given equipment, system or facility as required for input to the risk assessment process.
6. Validating the risk assessment process by addressing selected equipments, systems and facilities
7. Performing risk assessments of both U.S. INFOSEC equipments and systems, and U.S. facilities using U.S. INFOSEC equipments and systems.
8. Developing and maintaining a risk management system which would include, but not be limited to, a vulnerability database, a database of U.S. INFOSEC equipments and systems with vulnerabilities and their corporate resolutions, and a database of U.S. facilities that use U.S. INFOSEC equipments and systems with vulnerabilities and their countermeasures.
9. Preparing and presenting the annual Security Status of INFOSEC Equipments and Systems Report to the ISSO corporate management.
10. Performing the necessary research risk analysis, modeling and related areas in support of the mission.
11. Developing or obtaining the automated tools that are necessary for developing and maintaining the threat models and the risk assessment process.
12. Preparing technical reports and briefings to document the risk assessments and the threat models.

**FOR OFFICIAL USE ONLY**

# UNCLASSIFIED

## Technical Assessment File

This file contains INFOSEC risk assessment reports and technical papers regarding information systems.

DATE SPAN: 1986 to Present  
LOCATION: C82  
STORAGE MEDIA: Paper  
VOLUME: 1 cu. ft. per year  
CLASSIFICATION: TOP SECRET CODEWORD NOFORN  
DISPOSITION: Permanent. Transfer to NCRC when no longer needed for operations.  
DISPOSITION NO. n C82-1

## Administrative File

This file contains general office administration records as well as a record of correspondence.

DATE SPAN: 1986 to Present  
LOCATION: C82  
STORAGE MEDIA: Paper  
VOLUME: 1 cu. ft. per year  
CLASSIFICATION: SECRET  
DISPOSITION: Destroy when 3 years old or when no longer required for operations. (001B) (GRS 23-1)  
DISPOSITION NO.: C82-2

UNCLASSIFIED

**UNCLASSIFIED**

**C83**  
**SYSTEM**  
**SERVICES**

**UNCLASSIFIED**

## System Services

The Chief of the System Services Division is responsible to the Chief of the Office of INFOSEC Standards, Assessments, and System Services for planning Airport Square 11's operational ADP requirements; developing and maintaining the NCSC's ADP support activities and resources; establishing and operating NSA's DOCKMASTER computer center facility; establishing and supporting local area networks (LANs); developing and maintaining special ADP applications; developing and monitoring the FINPLAN Build for C8; and maintaining equipment inventory for Airport Square 11.

Primary functions include:

1. Acquiring, developing, and maintaining systems in support of C and the NCSC's management, project management, and information services functions.
2. Acquiring, managing, and maintaining special computer security applications using existing technology.
3. Managing, operating, and maintaining the DOCKMASTER computer center.
4. Planning, budgeting, and executing procurement RDT&E, and O&M budgets in support of C8 operations.
5. Providing computer systems services (DOCKMASTER) to the U.S. Computer Security Community.
6. Acquiring, managing, and maintaining software security tools for use in C Group's computer security evaluations and research tasking. Coordinating with other evaluation and artificial intelligence efforts in government, and the private sector for purposes of information sharing and maintenance of technical proficiency.

# UNCLASSIFIED

## Graphics Library System Data Base

This data base is used to store data pertaining to text and identification information on slides used for NCSC briefings.

DATE SPAN: 1985 to Present

LOCATION: C83

STORAGE MEDIA: Hard Disk

HARDWARE: Honeywell DPS (DOCKMASTER) 8/70 M

SOFTWARE: MRDS (LINUS)

VOLUME: 1,500 logical records (300 per yr)

CLASSIFICATION: UNCLASSIFIED

DISPOSITION: Delete or destroy data when no longer needed for operations.

DISPOSITION NO.n C83-1

## Mailing and Conference System (MACS) Data Base

This data base is used to provide names for Center-wide mailings of computer security related information and attendees to the National Computer Security Conference.

DATE SPAN: 1983 to Present

LOCATION: C83

STORAGE MEDIA: Hard Disk

HARDWARE: Honeywell DPS 8/70 M (DOCKMASTER)

SOFTWARE: MRDS (LINUS)

VOLUME: 1,000 logical records per yr.

CLASSIFICATION: UNCLASSIFIED

DISPOSITION: Delete or destroy data when no longer needed for operations.

DISPOSITION NO.n C83-2

UNCLASSIFIED

# UNCLASSIFIED

## Administrative File

This file contains documentation relevant to operational management of the organization, including all facets of personnel administration, project management, and budget matters required to fulfill assigned missions and functions.

DATE SPAN: 1985 to Present

LOCATION: C83

STORAGE MEDIA: Paper

VOLUME: 10 cu. ft.

CLASSIFICATION: TOP SECRET CODEWORD

DISPOSITION: A. Personnel- Destroy 1 year after transfer or separation of employee. (003-1) (GRS 1-18a)

B. Budget:  
OPI- Permanent. Close annually. Transfer to the NCRC when no longer required for operations.

C. Budget:  
All others- Close annually. Transfer to the NCRC. Destroy when 10 years old or sooner if no longer required for operations. (002D-2)

DISPOSITION NO.: C83-3 A, B and C

UNCLASSIFIED

# UNCLASSIFIED

## Purchase Request File

This file contains purchase requests for hardware, software, and maintenance materials associated with C operations.

DATE SPAN: 1985 to Present

LOCATION: C83

STORAGE MEDIA: Paper/Disk

HARDWARE:

SOFTWARE:

VOLUME: 9 cu. ft./1 disk pack

CLASSIFICATION: SECRET

DISPOSITION: Destroy when terminated or completed.  
(GRS 3-3c)

DISPOSITION NO.e C83-4

UNCLASSIFIED

# UNCLASSIFIED

## Honeywell Multics Operational System Instructions File

This file contains detailed documentation relevant to the use of the Honeywell system.

DATE SPAN: 1983 to Present  
LOCATION: C83  
STORAGE MEDIA: Paper  
VOLUME: 24 cu. ft.  
CLASSIFICATION: UNCLASSIFIED  
DISPOSITION: Retain by OPI until no longer required for operations.  
DISPOSITION NO.: C83-5

### \*Network Users Administrative File

This file contains network users data.

DATE SPAN:  
LOCATION: C834  
STORAGE MEDIA: Paper/Disk  
HARDWARE: XEROX 6085- DOCKMASTER  
SOFTWARE: VIEWPOINT  
VOLUME: 10 cu. ft./1 disk pack  
CLASSIFICATION: TOP SECRET CODEWORD  
DISPOSITION: A. Paper- Delete or destroy after 3 years or when no longer required for operations. (GRS 23-1)  
B. Disk- Delete or destroy when superseded or obsolete.  
DISPOSITION NO.: C83-6 A and B

UNCLASSIFIED

**C9**  
**INFOSEC**  
**FIELD**  
**EVALUATION**

**FOR OFFICIAL USE ONLY**

INFOSEC Field Evaluation

The Chief, C9 is responsible to the Chief, C for evaluating fielded INFOSEC systems and networks, fielded INFOSEC products and equipment, secure facilities, and countermeasures, and for COMSEC monitoring. The Chief, C9 is also responsible for the development of techniques and technology to support the evaluation and monitoring mission; for the preparation of the consolidated NSA Technical Security (TECHSEC) program; for development of technical security policy and plans; for supporting the development of technical security and field evaluation standards, guidelines and specifications; for management of technical security and technical countermeasures operations; and for providing NSA leadership, representation and services to the technical security community.

Primary functions include:

1. Inspecting, testing, and evaluating secure communications and information processing products, equipment, systems, networks, facilities, and countermeasures.
2. Performing COMSEC monitoring, signal analysis, and traffic analysis to identify telecommunications vulnerabilities.
3. Planning, reviewing, and conducting technical security and technical counterintelligence operations to search for, detect, and counter foreign technical exploitation of secure communications, and information processing products, equipment, systems, networks, and facilities.
4. Developing techniques, technologies, and instrumentation for evaluation of secure communications and information processing products, equipment, systems, networks, facilities, and countermeasures.
5. Providing design and countermeasures support for secure communications and information processing products, equipment, systems, networks and facilities.
6. Serving as the ISSO point of contact and center of expertise for technical security.

~~SECRET~~

7. Providing NSA leadership and representation in various technical security forums (including the NTISSC Community and the Intelligence Community) and technical-security advice, assistance and services to the Intelligence Community and to other U.S. and foreign government agencies and departments.
8. Developing technical security policy and plans.
9. Supporting the development of technical security and field evaluation standards, specifications, guidelines, and assessments.
10. Managing technical security and COMSEC monitoring and analysis planning, resources, tasking, reporting, control measures, and coordination with NSA elements and U.S. Government departments and agencies.
11. Managing the reevaluation program for fielded INFOSEC products and equipment.

~~SECRET~~

# UNCLASSIFIED

## \*Tempest Advisory Group Subject Files

This file contains records pertaining to the organization and function of the Tempest Advisory Group. Subjects include: historical documents, meeting minutes, incoming and outgoing correspondence, documents related to publication, transmittals, administration of the TAG, and predecessor files (CAP)n

DATE SPAN: 1984 to Present

LOCATION: C9

STORAGE MEDIA: Paper/Disk/Slides

VOLUME: 3 cu. ft.

CLASSIFICATION:

DISPOSITION: Delete or destroy when no longer required for operations.

DISPOSITION NO.n C9-1

UNCLASSIFIED

# UNCLASSIFIED

## Administrative File

This file contains incoming and outgoing correspondence, reports, viewgraphs, and copies of manuals relating to general office administration.

DATE SPAN: 1982 to Present

LOCATION: C9

STORAGE MEDIA: Paper (data base under development)

HARDWARE: IBM

SOFTWARE: M204

VOLUME: 22 cu. ft.

CLASSIFICATION: TOP SECRET CODEWORD NOFORN

DISPOSITION: Destroy when 3 years old or when no longer needed for operations, whichever is sooner. (GRS 23-1)

DISPOSITION NO: C9-2

UNCLASSIFIED

C903  
INFOSEC  
FIELD  
EVALUATION  
SENIOR TECHNICAL STAFF

**FOR OFFICIAL USE ONLY**

C903

INFOSEC Field Evaluation Senior Technical Staff

The C903 technical staff is responsible to the Chief, C9 for providing senior-level technical direction and guidance in all phases of evaluations of fielded INFOSEC systems and networks, fielded INFOSEC products and equipment, secure facilities and countermeasures; and in COMSEC monitoring.

Primary functions include:

1. Anticipating vulnerabilities of fielded INFOSEC systems and networks, fielded INFOSEC products and equipment, secure facilities and countermeasures.
2. Identifying the need for and conducting research in the development of future fielded evaluation and COMSEC monitoring techniques and instrumentation.
3. Supporting the development of evaluation standards to assess the security of fielded INFOSEC products, equipment, systems and networks.
4. Integrating the staff's cumulative technical expertise across the C9 senior technical staff and across the technical work centers within C9.
5. Developing and encouraging individuals in the C9 technical work force to expand their knowledge and interaction with other parts of C9 and elsewhere to create an integrated INFOSEC field evaluation capability.

C91  
FIELDDED  
INFOSEC SYSTEM  
AND  
NETWORK  
EVALUATION

**FOR OFFICIAL USE ONLY**

C91

Fielded INFOSEC System and Network Evaluation

The Chief, C91, is responsible to the Chief, C9 for evaluating fielded INFOSEC computers, networks, and systems; providing technical INFOSEC evaluation support to operational system managers and system accreditors in the evaluation of fielded systems processing classified and/or sensitive information; and managing the inspection of equipment of out of U.S. control and equipment returned from the field.

Primary functions include:

1. Evaluation of fielded INFOSEC computers, networks, and systems.
2. Providing guidance and/or assistance in correcting noted deficiencies in evaluated fielded INFOSEC systems.
3. Making recommendations to the appropriate decision authorities regarding operational use of evaluated INFOSEC systems.
4. Providing support for security risk assessments for fielded INFOSEC systems.
5. Developing field evaluation techniques, technology, procedures, and instrumentation.
6. Supporting the development of evaluation standards to assess the security of fielded INFOSEC computers, networks and systems.
7. Assisting accreditors of evaluated systems by providing evaluation results to configuration control boards to facilitate the reaccreditation and reevaluation program for fielded INFOSEC systems.
8. Assisting DOD in the development of its evaluation of fielded INFOSEC computers, networks and systems.
9. Participating in joint INFOSEC field evaluation efforts with appropriate Intelligence Community and NTISS Community members.

~~SECRET~~

10. Evaluating fielded NATO and other foreign computers and networks.
11. Managing the inspection of equipment out of U.S. control and equipment returned from the field.

~~SECRET~~

# UNCLASSIFIED

## Travel Data Base

This data base is used to track TDY expenditures for C91. It is also used in compiling budgets each fiscal year.

DATE SPAN: 1989 to Present  
LOCATION: C91  
STORAGE MEDIA: Hard disk  
HARDWARE: PC  
SOFTWARE: DB III  
VOLUME: 10k bytes  
CLASSIFICATION: TOP SECRET  
DISPOSITION: Destroy when 3 years old or sooner if no longer needed for operations. (GRS 23-1)  
DISPOSITION NO.: C91-1

### ~~Reports File~~ \*

~~This file consists of project correspondence and reports concerning the INFOSEC evaluation of Fielded Systems and networks. Reports are sent to the Technical Library.~~

~~DATE SPAN: 1983 to Present  
LOCATION: C91  
STORAGE MEDIA: Paper  
VOLUME: .8 cu. ft.  
CLASSIFICATION: TOP SECRET NOFORN  
DISPOSITION: Cut off annually. Destroy when 3 years old or sooner if no longer needed for operations. (GRS 23-1)  
DISPOSITION NO.: C91-2~~

*del C09-2*

\*~~Obsolete. No longer created. See 6/12/2014 email. MPB~~

UNCLASSIFIED

UNCLASSIFIED

~~BLACKER File \*~~

~~This file consists of project correspondence and reports concerning the promotion of COMSEC for advanced data networks, both commercial and governmentale Reports are sent to the Technical Librarye~~

~~DATE SPAN: 1983 to Present~~

~~LOCATIONe C91~~

~~STORAGE MEDIA: Paper~~

~~VOLUME: .8 cu. ft.~~

~~CLASSIFICATIONe TOP SECRET NOFORN~~

~~DISPOSITIONe Cut off annually. Destroy when 3 years old or sooner if no longer needed for operationse (GRS 23 1)~~

~~DISPOSITION NO.e C91-3~~

~~DELETEDe 26 NOVEMBER 1991~~

C91-3  
Blacker File.  
(C72-transfer?)

\*●bsolète. No longer created. See 6/12/2014  
email. MPB

UNCLASSIFIED

# UNCLASSIFIED

## Correspondence File

This file contains incoming and outgoing correspondence and memoranda related to C91's general office administration.

DATE SPAN: 1989- Present  
LOCATION: C91  
STORAGE MEDIA: Paper, magnetic disk  
VOLUME: .25 cu. ft.  
CLASSIFICATION: TOP SECRET NOFORN  
DISPOSITION: Destroy when 3 years old or sooner if no longer needed for operations. (GRS 23-1)  
DISPOSITION NO: C91-4

### ~~T Operating System (TOS) File\*~~

~~This file contains information concerning the COMPUSEC evaluation of the T Operating System. Reports are sent to the Technical Library.~~

~~DATE SPAN: 1985 to Present  
LOCATION: C91  
STORAGE MEDIA: Paper  
VOLUME: 2 cu. ft.  
CLASSIFICATION: TOP SECRET CODEWORD NOFORN  
DISPOSITION: Cut off annually. Destroy two years thereafter.  
DISPOSITION NO.: C91-5~~

\*Obsolete. No longer created. See 6/12/2014 email. MPB

UNCLASSIFIED

# UNCLASSIFIED

## Suspense Log Data Base

This data base is used to track the suspenses and to generate weekly reports on all active and overdue suspenses.

DATE SPAN: 1984 to Present

LOCATION: C94

STORAGE MEDIA: Disk

HARDWARE: PC

SOFTWARE: DB III

VOLUME:

CLASSIFICATION: TOP SECRET

DISPOSITION: Destroy when 3 years old or sooner if no longer required for operationsn (GRS 23-1)

DISPOSITION NO.e C91-6

UNCLASSIFIED

**UNCLASSIFIED**

**C92  
COMSEC  
MONITORING  
AND  
ANALYSIS**

**UNCLASSIFIED**

C92

COMSEC Monitoring and Analysis

The Chief, C92, is responsible for performing COMSEC monitoring, signals and traffic analysis of U.S. Government telecommunications systems to identify vulnerabilities.

Primary functions include:

1. Developing and maintaining capabilities and resources to perform COMSEC monitoring and analysis of U.S. Government telecommunications systems from an adversary exploitation standpoint.
2. Monitoring U.S. Government telecommunications systems in support of NSA and external Department and Agency requirements.
3. Performing signals and traffic analysis and associated technical studies of U.S. Government telecommunications systems.
4. Identifying and reporting vulnerabilities of U.S. Government telecommunications systems to organizations which have the capability to remedy them.
5. Evaluating the effectiveness of INFOSEC applications or systems against specific vulnerabilities.
6. Managing NSA COMSEC monitoring and analysis resources, providing planning, tasking, reporting, control and coordination within NSA and U.S. Government Departments and Agencies.
7. Developing techniques, technology and instrumentation to support COMSEC monitoring and analysis.

# UNCLASSIFIED

## Administrative File

This file contains pertinent documentation relevant to the administrative management of the C92 organization, to include personnel administration, training, procurement, security, travel, budget and planning required to fulfill missions and functions.

DATE SPAN: 1988-Present

LOCATION: C92

STORAGE MEDIA: Paper/Diskettes

HARDWARE: XEROX STAR

SOFTWARE: XEROX OA/VIEWPOINT

VOLUME: 7 cu ft.

CLASSIFICATION: TOP SECRET CODEWORD

DISPOSITION: A. Personnel Records: Destroy 1 year after separation or transfer of employee (GRS 1-18a)

B. Administrative Records: Destroy after 3 years or when no longer needed for operations, whichever is sooner

C. Correspondence File: Cut off annually  
Destroy after 3 years

DISPOSITION NO: C92-1 A, B and C

UNCLASSIFIED

# UNCLASSIFIED

## Procurement Request File

This file contains all procurement requests for equipment to support C92 COMSEC collection and analysis activities.

DATE SPAN: 1987 to Present

LOCATION: C92

STORAGE MEDIA: Paper/Floppy Disk

HARDWARE: PC-XT/XEROX STAR/MARMOSET PC-II

SOFTWARE: PFS/VIEWPOINT/INGRES

VOLUME: 1 cu. ft./200 records (100 per year)

CLASSIFICATION: SECRET

DISPOSITION: Destroy upon termination or completion.  
(GRS 3-3)

DISPOSITION NO.: C92-2

UNCLASSIFIED

# UNCLASSIFIED

## Signals File

This file contains records pertaining to a variety of subjects including adversary SIGINT targeting, COMSEC vulnerability assessments, satellites, noncommunications signals, foreign signals, threats, jamming, and the Worldwide Airborne Command Post.

DATE SPAN: 1980 to Present

LOCATION: C92

STORAGE MEDIA: Paper/Microfiche (COMSEC vulnerability assessments MCN NSA-91-S-C92001)

VOLUME: 2 cu. ft.

CLASSIFICATION: TOP SECRET CODEWORD, NOFORN

DISPOSITION: Permanent. Cut off annually. Transfer to NCRC when no longer required for operations.

DISPOSITION NO.: C92-3

UNCLASSIFIED

## Operations File

This file contains records pertaining to COMSEC Operations including station profiles, communications nets, systems, monitoring and analysis, and COMSEC procedures.

DATE SPAN: 1980 to Present  
LOCATION: C92  
STORAGE MEDIA: Paper  
VOLUME: 3 cu. ft.  
CLASSIFICATION: TOP SECRET CODEWORD, NOFORN  
DISPOSITION: Permanent. Transfer to NCRC when no longer required for operations.  
DISPOSITION NO.e C92-4

### ~~Electromagnetic Compatibility Analysis Center (ECAC) File \*~~

~~This file contains listings of U.S., DoD and civil government agencies. Includes locations, equipments, organizational designators, and computer information.~~

~~DATE SPAN: 1980 to Present  
LOCATION: C923  
STORAGE MEDIA: Hard Disk  
HARDWARE: MARMOSET PC II  
SOFTWARE: MARMOSET - INGRES  
VOLUME: 1 million records  
CLASSIFICATION: SECRET CODEWORD, NOFORN  
DISPOSITION: Destroy when no longer needed for operations.  
DISPOSITION NO.n C92-5  
DELETEDn 20 NOV. 1991~~

\***●**obsolete. No longer created. See 6/12/2014 email. MPB

**FOR OFFICIAL USE ONLY**

# UNCLASSIFIED

~~SIGSEC Technical Analysis Report File \*~~

~~This file consists of frequencies and related technical characteristics of signals monitored by C92 RCMC's.~~

~~DATE SPAN: 1985 to Present~~

~~LOCATION: C923~~

~~STORAGE MEDIA: Magnetic Tape~~

~~HARDWARE: MARMOSET PC II~~

~~SOFTWARE: MARMOSET - INGRES~~

~~VOLUME: 1 cu.rft.~~

~~CLASSIFICATION: SECRETq NOFORN~~

~~DISPOSITION: Destroy when superseded, rescinded, or revised.~~

~~DISPOSITION NO.: C92-6~~

\*~~o~~bsolute. No longer created. See 6/12/201  
email. MPB

UNCLASSIFIED

## Adversary SIGINT Targeting Data Base

This data base contains information on adversary SIGINT targeting of U.S. Communications. The data base includes information on frequencies, dates and times, SIGINT platforms, report serials, and results of ECAC searches and direction finding. This data base contains information on projects ALLEGATOR, BLACKTAIL, GUNSHIP, TINDERBOX, and OUTBURST.

DATE SPAN: 1985 to Present

LOCATION: C924

STORAGE MEDIA: Magnetic Tape/Paper

HARDWARE: MARMOSET, PCII

SOFTWARE: UNIX

VOLUME: 3,500 Records/2 cu. ft.

CLASSIFICATION: SECRET CODEWORD, NOFORN

DISPOSITION: Destroy when superseded, revised, rescinded, obsolete, or when no longer needed for operations.

DISPOSITION NO.: C92-7

**FOR OFFICIAL USE ONLY**

# UNCLASSIFIED

## Assessment Data Base

This data base contains technical results of COMSEC assessments conducted by C92.

DATE SPAN: 1985 to Present  
LOCATION: C92  
STORAGE MEDIA: Magnetic Tape  
HARDWARE: MARMOSET, PCII  
SOFTWARE: UNIX, INGRES  
VOLUME: 1 cu.ft.  
CLASSIFICATION: TOP SECRET, NOFORN  
DISPOSITION: Permanentn Retained by OPI.  
DISPOSITION NO.n C92-8

## Equipment Data Base

This data base contains an inventory of C92 equipment.

DATE SPAN: 1983 to Present  
LOCATION: C92  
STORAGE MEDIA: Magnetic Tape  
HARDWARE: MARMOSET, PCII  
SOFTWARE: UNIX, INGRES  
VOLUME: 2 cu.ft.  
CLASSIFICATION: UNCLASSIFIED  
DISPOSITION: Destroy when superseded, revised, rescinded, obsolete, or when no longer needed for operations.  
DISPOSITION NO.n C92-9

UNCLASSIFIED

**UNCLASSIFIED**

**C93  
FACILITIES  
AND  
COUNTERMEASURES  
EVALUATION**

**UNCLASSIFIED**

C93

### Facilities and Countermeasures Evaluation

To conduct technical security evaluations of NSA and U.S. Government systems and facilities. Develop and evaluate new facility countermeasures and conduct evaluations of the effectiveness of existing facility countermeasures. Evaluate the application of technical security countermeasures to facilities. Conduct field evaluations of LPI/LPD systems. Develop techniques and tools which have specific applications to facility evaluation. Develop evaluation standards to judge the technical security of facilities. Provide technical security advice to various U.S. Government departments and agencies, NATO and other foreign governments. Manage the NSA TEMPEST security program.

Primary functions include:

1. Performing technical security evaluations of NSA and other U.S. Government facilities.
2. Developing new and evaluating new and existing facility countermeasures for effectiveness against technical security attacks.
3. Conducting field evaluations of LPI/LPD systems.
4. Developing techniques, technology and instrumentation to support facility, countermeasures and LPI/LPD system evaluation.
5. Developing evaluation standards to assess the security of facilities. Develop technical security procedures and techniques for facilities (e.g. incoming equipment verification, TEMPEST installation requirements, physical control measures, and shielding and isolation techniques).
6. Providing technical security facility guidance to U.S. Government departments and agencies, NATO and other foreign governments.
7. Managing the NSA and NSA SCI contractor TEMPEST security program.

Countermeasures Development File

This file contains information reflecting the research, development, design and fabrication of technical security countermeasures, tools ,and techniques to protect U.S. facilities.

DATE SPAN: 1985 to Present  
LOCATION: C93  
STORAGE MEDIA: Paper  
VOLUME: 25 cu. ft.  
CLASSIFICATION: TOP SECRET CODEWORD  
DISPOSITION: Permanent. Transfer to NCRC when no longer needed for operations  
DISPOSITION NO: C93-1

Technical Security Evaluation File

This file contains all reports, correspondence, and background materials related to technical security facility evaluations performed at NSA and U.S. facilities worldwide.

DATE SPAN: 1985 to Present  
LOCATION: C93  
STORAGE MEDIA: Paper  
VOLUME: 25 cu. ft.  
CLASSIFICATION: TOP SECRET CODEWORD  
DISPOSITION: Permanent. Transfer to NCRC when no longer needed for operations.  
DISPOSITION NO: C93-2

**FOR OFFICIAL USE ONLY**

Correspondence File

This file contains incoming and outgoing letters, memoranda, reports, messages, and related records reflecting technical security functions, programs, and planning.

DATE SPAN: 1980 to Present  
LOCATION: C93  
STORAGE MEDIA: Paper  
VOLUME: 10 cu. ft.  
CLASSIFICATION: TOP SECRET  
DISPOSITION: Cut off annually. Destroy 3 years thereafter.  
(001A-3) (GRS 23-1)  
DISPOSITION NO: C93-3

NSA/SCIF TEMPEST Program File

This file contains documents relating to the National TEMPEST policy and the NSA TEMPEST Program. Included is material concerning TEMPEST certification for NSA controlled Sensitive Compartment Information Facilities (SCIFs)

DATE SPAN: 1965 to Present  
LOCATION: C93  
STORAGE MEDIA: Paper  
VOLUME: 14 cu. ft.  
CLASSIFICATION: TOP SECRET  
DISPOSITION: A. Policy and Program Records Permanent. Transfer to NCRC when no longer needed for operation.  
~~B. All Other Records Cut off annually. Destroy when five years old.~~ \*  
DISPOSITION NO: C93-4 A and B

\*●bsolute. No longer created. See 6/12/2014  
email. MPB

**FOR OFFICIAL USE ONLY**

~~Security Data Base \*~~

~~This data base is used to track the security of NSA facilities and equipment worldwide. As a supplement to Technical Security Evaluation Files, it is used to track dates, names, phone numbers and related items pertaining to inspections.~~

~~DATE SPAN: Under development~~

~~LOCATION: C93~~

~~STORAGE MEDIA: Hard disk~~

~~HARDWARE: IBM 370 (RAPPER)~~

~~SOFTWARE: M204~~

~~VOLUME:~~

~~CLASSIFICATION: TOP SECRET CODEWORD~~

~~DISPOSITION: Delete or destroy when no longer needed for operations.~~

~~DISPOSITION NO.: C93-5~~

~~DELETED: 20 NOV. 1991~~

\*~~●~~obsolete. No longer created. See 6/12/2014 email. MPB

**FOR OFFICIAL USE ONLY**

**UNCLASSIFIED**

**C94  
POLICY,  
PLANNING  
AND  
MANAGEMENT  
SUPPORT**

**UNCLASSIFIED**

~~SECRET~~

C94

Policy, Planning and Management Support

The Chief of C94 is responsible to the Chief, C9 for technical security and fielded systems evaluation program planning, policy, operations planning, foreign relations, classification guidelines, U.S. Government community and foreign liaison, resource management, administrative management, and operation of the National TEMPEST Information Center.

Primary functions include:

1. Planning the use of technical security and field evaluation resources.
2. Managing the execution of technical security and field evaluation funds.
3. Preparing the consolidated NSA Technical Security Program.
4. Recommending technical security policies within NSA and the U.S. Government.
5. Coordinating C9 actions and developing C9 plans and policies regarding foreign governments.
6. Planning and coordinating special technical security and countermeasures operations and effecting interagency approval.
7. Supporting the development of new and updating of existing technical security and field evaluation standards, guidelines, and specifications.
8. Coordinating and supporting C9 leadership, representation and participation in technical security forums within NSA and the U.S. Government and with foreign governments.
9. Supporting the operation of a national TEMPEST training program.
10. Arranging training support to the technical security community.

~~SECRET~~

~~SECRET~~

11. Monitoring and reporting technical security incidents.
12. Maintaining databases in support of planning, development, evaluation, reports, resources, and operations.
13. Establishing controls on release of technical security information; conducting classification reviews.
14. Monitoring service contract and national laboratory tasking and reporting.
15. Operating the National TEMPEST Information Center.
16. Managing all C9 personnel and administrative actions.

~~SECRET~~

# UNCLASSIFIED

## Subject File

This file includes incoming and outgoing correspondence, budget and contract information, point papers, foreign contacts, and background information pertaining to Technical Security Evaluations.

DATE SPAN: 1982 to Present

LOCATION: C94a

STORAGE MEDIA: Paper

VOLUME: 3 cu. ft.

CLASSIFICATION: TOP SECRET NOFORN

DISPOSITION: Close annually. Destroy after 3 years or sooner if no longer required for operations.  
(GRS 23-1)

DISPOSITION NO. C94-1

UNCLASSIFIED

# UNCLASSIFIED

## National TEMPEST Information Center Library

This file contains TEMPEST documents related to standards, test plans and test reports for commercial and governmental cryptoequipment.

DATE SPAN: 1958 to Present

LOCATION: C941

STORAGE MEDIA: Paper, magnetic disk, magnetic tape, slides, photographs, microform

HARDWARE: Mainframe (HP 1000)

SOFTWARE: Fortran

VOLUME: 63.5 cu. ft. (4 disks and 56 1600 bpi magnetic tapes)

CLASSIFICATION: TOP SECRET NOFORN

DISPOSITION: Permanent. Transfer to NCRC when no longer needed for operations.

DISPOSITION NO: C94-2

UNCLASSIFIED

# UNCLASSIFIED

## Administrative File

This file contains records relating to the administrative management of the organization in areas such as personnel administration, budget matters and security which are required to fulfill assigned missions and functions.

DATE SPAN: 1987 to Present

LOCATION: C94

STORAGE MEDIA: Paper

VOLUME: 6 cu. ft.

CLASSIFICATION: TOP SECRET CODEWORD, NOFORN, VRK

DISPOSITION: A. Personnel Records: Destroy 1 year after separation or transfer of employee. (GRS 1-18a)

B. Administrative Records: Retain for 3 years and thereafter destroy. (GRS 23-1)

DISPOSITION NO.e C94-3A and B

## Threat File

This file contains a history of known exploitation of information processing equipment/systems.

DATE SPAN: 1972 to Present

LOCATION: C94

STORAGE MEDIA: Paper

VOLUME: 3 cu. ft.

CLASSIFICATION: TOP SECRET CODEWORD, NOFORN, VRK

DISPOSITION: Permanent. Transfer to NCRC when no longer required for operations.

DISPOSITION NO.: C94-4

UNCLASSIFIED

# UNCLASSIFIED

## Technical File

This file contains programs and operational data.

DATE SPAN: 1987 to Present  
LOCATION: C94  
STORAGE MEDIA: Paper  
VOLUME: 6 cu. ft.  
CLASSIFICATION: TOP SECRET CODEWORD, NOFORN, VRK  
DISPOSITION: Permanent. Retain in office 5 years. Transfer to NCRC.  
DISPOSITION NO.: C94-5

## Program/Project File

This file contains individual analyst project/current operation records.

DATE SPAN: 1987 to Present  
LOCATION: C94  
STORAGE MEDIA: Paper  
VOLUME: 39 cu. ft.  
CLASSIFICATION: TOP SECRET CODEWORD, NOFORN, VRK  
DISPOSITION: Permanent. Transfer to NCRC when no longer required for operations.  
DISPOSITION NO.: C94-6

UNCLASSIFIED

~~TOP SECRET~~

~~HANDLE VIA COMINT CHANNELS ONLY~~  
~~TOP SECRET~~

Redactions have been made to this report pursuant to 5 U.S.C. 552(b)(3) with the corresponding statute 50 USC § 3605 (Previously 50 U.S.C. 402, noting National Security Agency Act of 1959) , which protects from disclosure “information pertaining to the functions or organization of NSA and certain information pertaining to NSA employees.” You will need to submit a Freedom of Information Act (FOIA) request to the Office of the General Counsel for the withheld information. Information on how to file a FOIA may be found here:

<http://www.archives.gov/foia/>