~~SECRET~~

DRAFT

15 March 1985

COMMAND & CONTROL
SYSTEMS ORGANIZATION

CHOSUN NETWORK SECURITY MANUAL (U)

CLASS. BY: DCA184W00224 DECLASSIFY ON: OADR	REQUESTS FOR THIS DOCUMENT MUST BE REFERRED TO:	CCSO CY OF CYS

DRAFT

~~SECRET~~

SECRET

DRAFT

15 March 1985

COMMAND & CONTROL
SYSTEMS ORGANIZATION

CHOSUN NETWORK SECURITY MANUAL (U)

CLASS. BY: DCA184W00224 DECLASSIFY ON: OADR	REQUESTS FOR THIS DOCUMENT MUST BE REFERRED TO:	CCSO CY OF CYS

DRAFT

SECRET

CONTENTS

ILLUSTRATIONS

SECTION 1. INTRODUCTION (U)

1.1 General (U)

(S) The CHOSUN network is designed to improve the nation's crisis management capability in support of the President. To facilitate this objective, the CHOSUN network will provide an audio/video teleconferencing capability that will permit senior officials of the Executive Branch to communicate freely and candidly during crisis situations in an environment that approximates face-to-face meetings.

(S) During crisis situations, the CHOSUN network will communicate information of a highly sensitive nature from the White House to participating agencies. In the interest of national security, the network will provide extraordinary protective features to safeguard the security and privacy of information communicated and to avoid proliferation of knowledge about the configuration and capabilities of the network. Multiple security measures to safeguard information will include the continuous employment of protective features in the hardware and software design configuration as well as procedural and technical controls in the areas of personnel, physical, emanations, and communications security.

(U) Continuing operation of the CHOSUN network will be contingent upon the results of a continuing review, test, and favorable evaluation of the security features of the network, including unannounced evaluations of the security posture of each of the CHOSUN nodes.

(S) The Assistant to the President for National Security Affairs is the Designated Approving Authority (DAA) for the CHOSUN network, with sole authority to approve or disapprove the security and privacy features of the CHOSUN network and accredit the network for operation with classified information.

1.2 Purpose (U)

(U) This security manual provides the basic policy, criteria, techniques, and procedures to implement, certify, accredit, operate, and maintain the CHOSUN network.

1.3 Applicability and Scope (U)

(S) This security manual applies to all Executive Branch agencies which develop, operate, maintain, or use the CHOSUN network. It also applies to all contractors and/or private individuals who develop, operate, maintain, or use the CHOSUN network. The provisions of this security manual are binding. Conformance is not discretionary.

1.4 Authority (U)

(C) This policy is established in accordance with the provisions of National Security Decision Directive 95, the National Security Act of 1947, and Executive Order 12356.

1.5 Amendments (U)

(U) All amendments or updates to this security manual will be published, as necessary, by the Network Security Officer (NSO) of the CHOSUN network. Proposed amendments or updates may be forwarded under agency-head signature to the NSO.

1.6 Reproduction (U)

(S) Reproduction of this manual is not authorized. Additional copies may be requested from the National Security Council (NSC) in writing. The request must include the name of the accountable individual and the full address of the recipient organization.

1.7 Definition of Terms (U)

(U) To avoid misunderstanding due to ambiguity of terms, definitions for selected terms used in this manual are provided in appendix A.

1.8 References (U)

(U) A list of documents used in the preparation of this manual is provided as appendix B.

SECTION 2. STATEMENT OF POLICY (U)

2.1 General (U)

(U) The following subsections present specific policy statements pertaining to all aspects of the CHOSUN network. These policies establish mandatory requirements designed to ensure the security of all information transmitted, stored, or processed by the network.

2.2 Appointment of the Designated Approving Authority (U)

(S) The Assistant to the President for National Security Affairs will be the Designated Approving Authority for the CHOSUN network. The DAA is responsible for providing official approval for the initial and continued operation of the CHOSUN network, based on continuing certification that all elements of the CHOSUN network meet the mandatory requirements of this security manual. The responsibilities of the DAA are specified in detail in section 3.

2.3 Network Operation (U)

(U) No element of the network (node or hub) will be operational without certification and accreditation in accordance with the provisions identified in section 4.

2.4 Network Security Organization and Structure (U)

(S) The Designated Approving Authority will provide for the appointment of the CHOSUN Network Security Officer to manage the implementation of security and the testing and evaluation of the security features of the CHOSUN network. The Network Security Officer will appoint and chair a Network Certification Working Group (NCWG), with members from the following agencies:

a. (U) National Security Agency.

b. (U) Central Intelligence Agency.

c. (U) Federal Bureau of Investigation.

d. (U) Department of Justice.

e. (U) United States Secret Service.

The responsibilities of the NSO are detailed in section 3. Additionally, the organizations operating the hub and each node will nominate individuals for DAA approval to serve as Information System Security

Officers for their respective sites. The responsibilities of the Hub Information System Security Officer (HISSO) and the Node Information System Security Officer (NISSO) are provided in detail in section 3.

2.5 Dissemination of Project CHOSUN Information (U)

(C) Since the CHOSUN network deals with crisis management decision-making at the national level, the dissemination of information about the network must be stringently controlled. Accordingly, a Security Classification Guide has been prepared for Project CHOSUN. A copy of this guide is provided as appendix C. The information security requirements for Project CHOSUN are identified in section 7, Information Security.

(C) The CHOSUN Security Classification Guide provides basic guidance for determining (1) the security classification, (2) schedules for downgrading, or (3) review of downgrading of Project CHOSUN information. The guide was formulated to protect from any adversaries sensitive information regarding the architecture, design, capabilities, and limitations of Project CHOSUN.

(C) Project CHOSUN-related information is the property of the National Security Council in the Executive Office of the President of the United States. Any release of this information, either classified or UNCLASSIFIED, to persons outside of the Executive Branch must be approved in writing by the NSO. All documents relating to Project CHOSUN will be marked "Property of the National Security Council. Written approval required for release."

(C) It must be assumed that hostile intelligence services have knowledge of and will target Project CHOSUN. Therefore, every effort must be made to protect information about its identity, system configuration, and capabilities. Knowledge about the CHOSUN network must not be proliferated.

2.6 Multiple Safeguards (U)

(U) The sensitivity of this system requires the application of every available safeguard to protect against the multidisciplinary hostile intelligence threat and to ensure the privacy of the officials utilizing the system. Multiple security measures and procedures will be used to attain an acceptable level of security. The CHOSUN network and the information transmitted within the network will be safeguarded by the continuous employment of protective features in the ADP system's hardware and software design and configuration, and by other appropriate information, physical, personnel, technical, and communications security controls.

2.7 Continuous Evaluation (U)

(U) The continued accreditation for the operation of the CHOSUN network is contingent upon the results of a continuing review and testing, including unannounced on-site inspections and favorable evaluation of the security features of the network.

2,8 Mode of Operation (U)

(U) Crisis management decisionmaking at the national level requires a diversity of information on an ad hoc basis from a variety of information sources. The information required ranges from the most highly classified Sensitive Compartmented Information (SCI) to UNCLASSIFIED information available from commercial sources, public data bases, and private individuals.

(U) The CHOSUN network must be capable of processing unclassified information as well as multiple levels of classified information within the framework of existing technology without sacrificing the security protection provided to classified information or restricting the flow of required information.

(C) In the near term, the required security will be achieved by operating the network, to include the hub switch and all connected nodes and node components, in the TOP SECRET/SCI system-high mode. The system-high mode is defined as the utilization of the system to process SCI information when the total network, to include the central hub facility, node processors, and connected components, is secured in accordance with the requirement for TOP SECRET information and for all categories of SCI processed, stored, or transmitted therein, and all users with access to the interconnected network have a valid TOP SECRET clearance and access approvals for all SCI stored, processed, or transmitted within the network.

(U) The desired long-term operational goal of the CHOSUN network is to operate in a controlled security mode where at least some users have neither a security clearance nor a need to know for all levels of classification and all types of SCI stored, processed, or transmitted within the network. The controlled mode will be achieved using hardware, software, and/or procedural security measures evaluated by the NCWG and approved by the DAA.

2.9 Summary of Security Requirements (U)

(U) The required security for the CHOSUN network will be provided by the continuous employment of the following protective features:

a. (C) Personnel Security - All U.S. Government employees, and contractor personnel, terminal operators, test and maintenance personnel assigned to Project CHOSUN must meet the requirements set forth in this document. The criteria and procedures shall be applied equally to all personnel. In addition, technical operators, U.S. Government and contractor personnel assigned to the CHOSUN hub will submit to polygraph testing.

b. (U) Physical Security - The physical security and certification requirements for a closed storage Sensitive Compartmented Information Facility (SCIF) as outlined in NFIB/NFIC-9.1/47 apply.

c. (U) Emanations Security (TEMPEST) - All equipment/systems associated with Project CHOSUN will either be installed within an RF-shielded room or installed in an RF-shielded cabinet/rack. The enclosures must meet NSA Specification 65-6, as specified and amended by appendix H. The TEMPEST guidelines for facility design and RED/BLACK installation outlined in NACSIM 5203 apply to the Project CHOSUN SCIF and the equipment/systems installed therein. Each Project CHOSUN SCIF must be certified prior to commencing classified operations. A request for facility certification using the format of Annex A of NSA/CSS Manual 90-5 must be completed by each agency/department and submitted to the NCWG.

d. (C) Communications Security:

(1) (U) Transmission Security - All Project CHOSUN circuits between the hub and each node shall be protected by a cryptographic key generator providing traffic flow security and operating 24 hours per day.

(2) (U) Cryptographic Security - All Project CHOSUN circuits between the hub and each node shall be protected by a Class A cryptographic system, specifically, the KG-81. End-to-end protection of data shall be accomplished using an NSA-approved Data Encryption Standard (DES) system which has been submitted to a Security Fault Analysis. The KG-81 and DES cryptographic periods shall be daily and per session, respectively.

(3) (U) Physical Security - The area in which cryptographic equipment is to be installed must meet the requirements set forth in this document and access to the area and the equipment must be restricted to

those personnel having a need to work. In those agencies/ departments administering a Cryptograph Clearance Program, each person requiring such access must hold a valid cryptographic clearance.

(4) (U) Network Security - All microprocessor-based telecommunications equipment/systems must be designed to prevent the spillage of data from one channel to another.

e. (U) ADP Security:

(1) (U) The hardware and software shall be developed, tested, and maintained in accordance with the provisions of Transmittal Memorandum No. 1 to OMB Circular No. A-71, as implemented in subsequent sections of this manual.

(2) (U) Hardware and software configuration management shall be in accordance with a Configuration Management Plan approved by the Network Certification Working Group.

(3) (U) The hardware/software shall provide the following security features:

(a) (U) The software shall clear user-inserted information stored on memory and hard disk and floppy disk storage at the start and termination of each conference or period of operation.

(b) (U) All individual users of network services, programs, or data must be identified and authenticated and their access request must be checked to ensure that it is authorized prior to establishing a connection between the user and the resource.

(c) (U) Each terminal shall be uniquely identified by the system. The system will have the capability of making a positive identification of each terminal prior to allowing that terminal to access system resources.

(d) (U) The security classification level and special access categories shall be identi-

fied with the information in the system, and appropriate labeling of any output shall be ensured.

(e) (U) The system shall produce, in a secure manner, an audit trail containing sufficient information to permit a regular security review of system activity. Audit trails shall be maintained at each node and at the hub.

(f) (U) The system shall provide a real-time facility to report security anomalies to a security monitor.

(g) (U) The system shall isolate user data from system control, net control, and technical control data.

SECTION 3. CHOSUN NETWORK SECURITY ORGANIZATION/RESPONSIBILITIES (U)

3.1 General (U)

(U) This section describes the tasks and responsibilities of all personnel involved in the development, implementation, operation, and maintenance of CHOSUN network security. Figure 3-1 presents an overview of the security organization hierarchy for the CHOSUN network.

3.2 Designated Approving Authority Responsibilities (U)

(U) The responsibilities of the DAA for the CHOSUN network are as follows:

a. (U) Accredit the CHOSUN network for initial or continued operation based upon review and evaluation of the appropriate system/network certification documents.

b. (U) Accredit all major modifications to the CHOSUN network.

c. (U) Approve the entry of each CHOSUN node into the CHOSUN network.

d. (U) Accredit each node and the hub for initial or continued operation based upon a review and evaluation of the appropriate node/hub certification documents.

e. (U) Make official decision for requiring nonscheduled network recertification/reaccreditation upon evaluating input of the NCWG.

f. (U) Appoint a CHOSUN NSO to manage the implementation of security and the testing and evaluation of the security features of the CHOSUN network.

g. (U) Authorize network access of all users of the CHOSUN network.

h. (U) Provide official approval of any changes to the security requirements of this manual, as recommended by the NCWG.

i. (U) Approve each node's interface with other ADP systems, terminals, or networks in order to ensure that these interfaces do not degrade the security of the CHOSUN network.

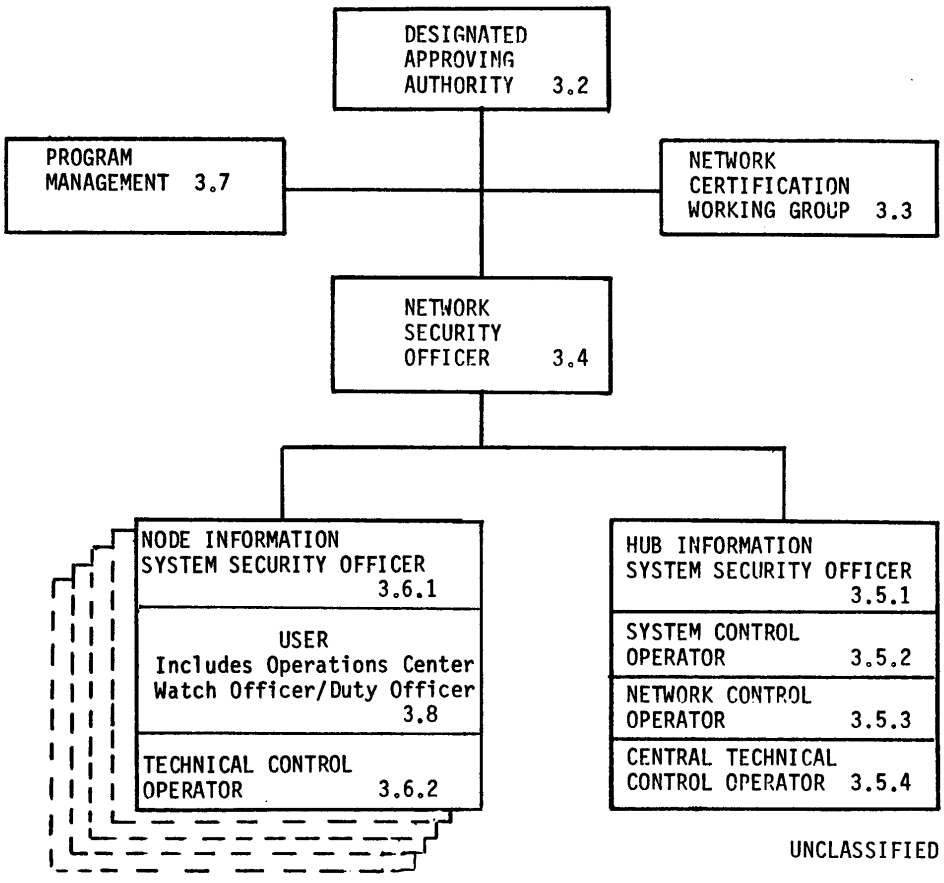


Figure 3-1. (U) CHOSUN Network Security Organization

3.3 Network Certification Working Group Responsibilities (U)

(U) The responsibilities of the NCWG are as follows:

a. (U) Perform certification/recertification for all nodes and the hub facility.

b. (U) Assess network-wide risk and perform periodic updates of the network threat.

c. (U) Review, evaluate, and consolidate the results of individual node and hub certifications and accompanying Security Test and Evaluation (ST&E) reports.

d. (U) Prepare a Network Security Report based on the network risk/threat analysis and individual ST&E reports.

e. (U) Review and evaluate all requests for waivers to the provisions of this manual and provide to the DAA as part of the node ST&E report all requests for waivers and a recommendation for approval if appropriate.

f. (U) Based upon the Network Security Report, certify/recertify the operational network and prepare a letter of network certification for forwarding to the DAA.

g. (U) Advise the NSO on matters pertaining to network security including a changing risk environment, or other changes in security policy, procedures, or technical criteria.

h. (U) Review and evaluate all network security incidents and violations and advise the DAA on the requirement/potential requirement for recertification or deactivation of the operational CHOSUN network.

i. (U) Participate in design reviews and validate the design of security protective features in the network.

j. (U) Review, evaluate, and recommend for approval each node's interface with other ADP systems, terminals, or networks, in order to ensure that these interfaces do not degrade the security of the CHOSUN network.

k. (U) Review, evaluate, and recommend for approval the procedures that are used by each node to disconnect elements of the node from the CHOSUN network, clear memory and disk storage, interconnect with other systems

processing information at a lower level, and store or destroy information in an approved mannner.

l. (U) Review, evaluate, and recommend for approval the procedures that are used by each node to reconnect elements back to the CHOSUN network after having been interconnected with other systems processing information at a lower level.

m. (U) Review, evaluate, and recommend for approval the configuration management procedures for the CHOSUN network as they relate to network security.

n. (U) Review and evaluate all proposed modifications to CHOSUN hardware/software elements for their security adequacy and inform the Network Configuration Manager of those items approved for installation.

o. (U) Based on results of testing by the Program Management Office, certify new system releases.

p. (U) Review and coordinate the Network Security Test Program.

q. (U) Review results and activities of the CHOSUN Network Test Team.

r. (U) Review, evaluate, and recommend for approval the security features of the network Standard Operating Procedures (SOP).

(C) The NCWG will initially be comprised of one representative from each of the following:

a. (U) National Security Agency.

b. (U) Central Intelligence Agency.

c. (U) Federal Bureau of Investigation.

d. (U) Department of Justice.

e. (U) United States Secret Service.

The CHOSUN NSO will serve as a voting member and chairman of the NCWG with authority to stop NCWG actions and present issues to the DAA. Where conflicts arise, the Chairman of the NCWG will act as sole interface to the DAA. The DAA will act as final arbiter for the

resolution of all issues relating to the security and privacy of the CHOSUN network.

3.4 Network Security Officer Responsibilities (U)

(U) The responsibilities of the NSO are as follows:

a. (U) Provide general supervision, administration, and overall coordination of CHOSUN network security matters, including operations, test and evaluation, certification, and accreditation.

b. (U) Prepare and disseminate all updates to the CHOSUN Network Security Manual.

c. (U) Ensure that security instructions, guidance, and SOPs are prepared, issued, and maintained for the network in accordance with DAA directions.

d. (U) Maintain cognizance of all aspects of network security including hardware, software, COMSEC, EMSEC, and all other considerations relating to network security.

e. (U) Review and monitor all proposed network or node configuration changes that may affect the security of the network or any user node, and forward recommendations to the NCWG for evaluation.

f. (U) Advise the Node Information System Security Officers (NISSOs) and Hub Information System Security Officer (HISSO) of scheduled outages for system testing or maintenance.

g. (U) Maintain a current library of network security documentation. This library will include but not be limited to:

(1) (U) CHOSUN Network Security Manual.

(2) (U) All technical references, standards, and criteria (current issues) required for certification of the CHOSUN network.

h. (U) Approve network/facility access authorization requests for all personnel other than user, forward user network access authorization requests to the DAA for approval.

i. (U) Maintain a security roster for all nonuser personnel approved for CHOSUN access, and assure system/network access permissions have been installed for authorized users.

j. (U) Ensure that personnel no longer requiring CHOSUN access are debriefed appropriately and that USERIDs/passwords are removed from the system when network users are debriefed.

k. (U) Advise NISSOs/HISSO on site-unique security matters.

l. (U) Develop and conduct a network/system security test program. Review and evaluate all test results, and provide any resultant recommendations for modifications to existing security procedures to the NCWG.

m. (U) Develop, conduct, and document a Security Training Program for the NISSOs and the HISSO.

n. (U) Perform a security review of all security incidents and related violations and provide immediate notification of all violations to the NCWG. If required, direct that a node be disconnected or that operation of the network be suspended.

o. (U) Serve as voting member [redacted] of the NCWG, in addition to being the NCWG chairman.

p. (U) Review and evaluate results of node/hub testing of contingency operations plans for security measures and modify security portions of the contingency operations plans as necessary. Forward proposed changes to the NCWG for approval.

3.5 Hub Security Elements (U)

3.5.1 (U) Hub Information System Security Officer Responsibilities. The responsibilities of the HISSO are as follows:

a. (U) Provide general supervision, administration, and overall coordination of network security matters for the hub, to include system control, network control, and central technical control elements.

b. (U) Serve as designated custodian for safeguarding all cryptographic equipment and materials (e.g., keying materials, manuals).

c. (U) Ensure that security instructions, guidance, manuals, and SOPs are implemented and maintained at the hub facilities.

d. (U) Notify the NSO of any security-related issues, activities, and incidents at the hub or within the operational network.

e. (U) Manage and assign responsibilitiy to the Central Technical Control Operator (CTCO), the Network Control Operator (NCO), and the System Control Operator (SCO) for testing and evaluation of hub/network features under their operational control.

f. (U) Inform the NSO of any proposed hardware or software changes within the hub.

g. (U) For personnel other than users, request network/facility access authorization/approval from the NSO (see section 5.4, Access Requests).

h. (U) Exercise contingency operations plans for the hub switch (see section 8.8). Results will be forwarded to the NCWG via the NSO for approval of the subject plan(s).

3.5.2 (U) System Control Operator Responsibilities. As the management element of the hub structure, the responsibilities of the SCO are as follows:

a. (U) Implement security instructions, guidance, and SOPs for the system control function.

b. (U) Maintain data results of routine security-related hardware/software functional and performance testing; this data should be retained for a period of six (6) months.

c. (U) Maintain data on all reported system/network security incidents; this data should be retained for a period of two (2) years.

d. (U) Act as alternate to the HISSO for safeguarding all cryptographic equipment and materials (e.g., keying materials, manuals).

3.5.3 (U) Network Control Operator Responsibilities. As an operational element of the hub structure, the responsibilities of the NCO are as follows:

a. (U) Implement security instructions, guidance, and SOPs for the network control function.

b. (U) Monitor network operational security and report incidents to the HISSO.

3.5.4 (U) Central Technical Control Operator Responsibilities. As an operational element of the hub structure, the responsibilities of the CTCO are as follows:

a. (U) Implement security instructions, guidance, and SOPs for the central technical control function.

b. (U) Provide operational control of cryptographic equipment and data encryption devices for the network.

c. (U) Monitor network security related to the technical control function and report incidents to the HISSO.

3.6 Node Security Elements (U)

3.6.1 (U) Node Information System Security Officer Responsibilities. The responsibilities of the NISSO are as follows:

a. (U) Provide general supervision, administration, and overall coordination of all security matters for the node.

b. (U) Ensure that security instructions, guidance, and SOPs are implemented and maintained at the node.

c. (U) Notify the NSO of any security-related issues, activities, and incidents at the node, including node outage reports.

d. (U) Manage and assign responsibility to the local Technical Control Operator (TCO) for testing of node/network features under his jurisdiction.

e. (U) Indoctrinate local users on applicable system/network security requirements and responsibilities prior to utilizing or accessing the network.

f. (U) Monitor and enforce physical access controls to the node facilities.

g. (U) Conduct daily routine checks of the Intrusion Detection System (see section 6.3).

h. (U) Provide for safeguarding all cryptographic equipment and materials (e.g., keying materials, manuals).

i. (U) Maintain a current access roster of all node personnel approved for CHOSUN access.

j. (U) Serve as Configuration Control Manager for the node, and thus inform the NSO of any proposed node changes.

k. (U) Immediately debrief departing personnel who have had access to the system/network, sending notification of departure and debriefing to the NSO.

l. (U) For users, request network/facility access authorization via the NSO; the NSO will forward each request to the DAA for approval. For all other personnel, request network/facility access authorization from the NSO (see section 5.4, Access Requests).

m. (U) Formulate and test contingency operations plans for the node system (see section 8.8).

n. (U) Prepare and forward to the NCWG for approval a node interface document which describes all node interfaces to the CHOSUN external ports.

o. (U) Prepare and forward to the NCWG all documentation of the procedures that will be used at the node to disconnect elements of the node from the CHOSUN network, clear the system, process at a lower classification level, and reconnect to the network.

3.6.2 (U) Technical Control Operator Responsibilities. The responsibilities of the TCO are as follows:

a. (U) Implement security instructions, guidance, and SOPs for the technical control functions.

b. (U) Monitor node security related to the technical control function and report incidents to the NISSO.

c. (U) Act as alternate to the NISSO for safeguarding all cryptographic equipment and materials (e.g., keying materials, manuals).

d. (U) Provide operational control of cryptographic equipment and data encryption devices for the node.

3.7 Program Management Responsibilities (U)

(U) The responsibilities of the Program Manager are as follows:

a. (U) Provide initial definition of the requirements for security features in the network.

b. (U) Retain the results of the design reviews as official records of the program; this data should be retained for a period of three (3) years.

c. (U) Document and retain the results of the security test as official records of the program.

d. (U) Develop the initial SOPs for the CHOSUN operational network.

3.8 User Responsibilities (U)

(U) All users of the network shall be briefed by the NISSO on the need for exercising sound security practices in protecting the information processed, stored, or transmitted by the network.

(U) As initiated by a transmitting node, the system software will provide the receiving node(s) with the audit elements appropriate to each data/audio/video conference (e.g., classification of conference, participants; see section 8.4, Audit Trails). The NISSO will ensure that the user(s) at the node is notified of the security mode in which the system is operating and the nodes (users) participating in the conference.

(U) At a minimum, originating users must:

a. (U) Be responsible for restricting distribution of data to those nodes having a legitimate need to know.

b. (U) Ensure that all input ADP products (e.g., printed listings, documents, hard-copy printouts of CRT displays) are marked in accordance with requirements prescribed for the highest level of classification of any information contained in the product.

(U) At a minimum, receiving users must:

a. (U) Immediately report to the NISSO the receipt of any ADP product not specifically requested or not marked with the appropriate security classification.

b. (U) Receipt for and protect all classified products transmitted by the network (see section 8.5.1.3, Control and Accountability).

THIS PAGE INTENTIONALLY LEFT BLANK

SECTION 4. CHOSUN NETWORK CERTIFICATION AND ACCREDITATION (U)

4.1 Objectives and Scope (U)

(U) This section describes the basic policy and procedures to be employed in the certification and accreditation of the CHOSUN network. The objective of the certification and accreditation process is to ensure that the CHOSUN network is developed, installed, operated, and maintained in accordance with requirements stated herein in order to provide adequate security protection.

(U) The process of certification and accreditation is of extreme importance in establishing and maintaining appropriate security safeguards within the CHOSUN network. Therefore, it must receive continuous attention, and be fully repeated at frequent intervals to assure adequate protection and safeguarding against any/all network changes and any/all environment changes.

(U) For purposes of clarity, the following definitions apply throughout this section:

a. (U) Certification is a technical evaluation of a subject network/system/subsystem demonstrating compliance with stated security requirements.

b. (U) Accreditation is approval or official authorization for a subject network/system/subsystem to handle sensitive information in an operational environment. As such, the accreditation process provides management control over security decisions and official acceptance of any residual risk.

4.2 Steps in CHOSUN Certification and Accreditation (U)

(U) Seven distinct elements are included within the certification and accreditation process for CHOSUN:

a. (U) Hardware/software certification.

b. (U) Node certification.

c. (U) Node accreditation.

d. (U) Hub certification.

e. (U) Hub accreditation.

f. (U) Network certification.

g. (U) Network accreditation.

Each element is briefly described below:

a. (U) Hardware/software certification provides a technical evaluation that all software (developmental and off-the-shelf) and hardware satisfy security requirements of the CHOSUN network. It is a composite evaluation based upon delivered documentation, results of various tests (contractor performed and independently confirmed by Government tests) and evaluation of the system in its proposed operating mode/environment. Hardware/software certification must be obtained before any CHOSUN system is approved for deployment to a CHOSUN facility.

b. (U) Node certification is the complete security evaluation or reevaluation of all CHOSUN components located within a node facility. Its scope encompasses all facets of ADP, personnel, physical, procedural, emanations, and communications security. It is based on the results of the node ST&E, Operational Test and Evaluation (OT&E), and a node risk analysis.

(U) While the major goal of the certification process is to evaluate technical compliance with stated security policy/requirements, it is recognized that in certain instances related to site-unique conditions within a node element, procedural compliance with a stated security requirement may be best accomplished in a manner different than specified herein. In no case will any security requirement be waived, but alternative approaches to requirement satisfaction may be considered on a very selective basis through a Request for Waiver.

(U) As part of the node certification process, the NCWG is responsible for identification of any security items not in strict compliance with this manual. For those items identified and subsequently evaluated and determined to be in noncompliance with the overall requirement, the user agency will document a Request for Waiver (appendix D) and include it in the Node ST&E report.

c. (U) Node accreditation is the formal approval for the node to initiate or continue operation within the CHOSUN network.

d. (U) Hub certification is the complete security evaluation/ reevaluation of all CHOSUN components located within the hub facility. Its scope encompasses the switching equipment, the control elements (network control, system control, technical control) and all related network equipment. Its scope encompasses hardware, software, personnel, procedures, emanations, and communications security, and is based upon a hub ST&E as well as operational testing performed with the nodes. A risk analysis for the hub must also be included in the ST&E report.

e. (U) Hub accreditation is the formal approval for the hub facility to initiate or continue operation within the CHOSUN network.

f. (U) Network certification for CHOSUN is the complete security evaluation or reevaluation of the entire CHOSUN network. Its scope encompasses all node facilities, the hub/switch, transmission system, network-level control elements, and network-level administrative and procedural security. It is based upon results from node certification, hub/switch certification, network-wide OT&E, and a rigorous, complete, network-wide security risk analysis.

g. (U) Network accreditation is the formal approval for initial or continued operation of the CHOSUN network. This approval authorizes the handling of classified information within the CHOSUN network, and also acknowledges official acceptance of any residual risk.

4.3 Hardware/Software Certification (U)

(U) All hardware/software intended for implementation within the CHOSUN network will be certified by the NCWG. This certification is based upon:

a. (U) Technical review and evaluation of contractor-developed documentation for developmental software.

b. (U) Technical review and evaluation of the integration technique for interfacing off-the-shelf software with developmental software.

c. (U) Technical review of contractor testing.

d. (U) Performance and review of an Independent Security Test (IST).

e. (U) Technical evaluation of the proposed hardware environment and associated operational procedures.

f. (U) A security risk analysis.

An ST&E report will be produced in order to provide documentation of items a through f above.

4.4 Node Certification (U)

(U) The certification of a CHOSUN user node encompasses all facets of telecommunications, personnel, physical, procedural, emanations, and communications security. The certification is based upon results of node OT&E and a node security risk analysis.

(U) The NCWG is responsible for certification of all nodes, and this process will be documented in a standardized ST&E Report; an ST&E report format is provided in appendix E. As part of the ST&E, the local NISSO must complete a security checklist, as shown in appendix F.

(U) In all cases where a node ST&E report contains at least one Request for Waiver, the NCWG may not certify the node until the Request for Waiver is formally reviewed by the DAA. Upon official approval by the DAA of the Request for Waiver, the NCWG will certify the node if all other requirements are satisfied. If a Request for Waiver is not approved by the DAA, the node personnel will take the necessary steps to provide acceptable compliance and revise the node ST&E report to reflect the actions taken. Requests for Waiver must not be considered as a routine part of a node's ST&E. Requests for Waiver will be approved only out of operational necessity and not for budgetary constraints.

4.5 Node Accreditation (U)

(U) The accreditation of a CHOSUN node provides official approval for that node to initiate or continue operations within the CHOSUN system. Accreditation for an individual node will be the responsibility of the DAA.

(U) Upon granting node certification, the NCWG will prepare a letter of certification to be included with the following items as part of the accreditation request package:

a. (U) The node ST&E Report.

b. (U) The node Security Manual.

c. (U) The (proposed) roster of node personnel to have CHOSUN access.

d. (U) The (proposed) node-unique information compartments to be handled by the CHOSUN system.

e. (U) Recommended waivers, if any.

(U) As a goal, node accreditation should be completed within 30 days of node certification.

4.6 Hub Certification (U)

(U) Certification for the hub facility will be the responsibility of the CHOSUN NCWG.

4.7 Hub Accreditation (U)

(U) Upon granting hub certification, the NCWG will prepare a letter of certification to be included with the following items as part of the accreditation request package:

a. (U) The hub ST&E Report.

b. (U) The hub Security Manual.

c. (U) The (proposed) roster of personnel working within the hub facility.

d. (U) Recommended waivers, if any.

(U) Accreditation of the hub facility is the responsibility of the DAA.

4.8 CHOSUN Network Certification (U)

(U) The CHOSUN network certification is the overall security evaluation/reevaluation of the entire CHOSUN network; as such, its scope includes the nodes, hub facility, transmission system, personnel, and procedures of the entire CHOSUN network. It relies extensively upon results of node/hub ST&Es.

(U) The NCWG will be responsible for the network certification process. Upon completion of the certification activities, a letter of certification will be prepared by the NCWG for the DAA. In addition, as part of the accreditation request package, the following items will be forwarded to the DAA:

a. (U) The CHOSUN Network Security Evaluation Report.

b. (U) The CHOSUN Network Security Manual.

c. (U) Specific identification of proposed nodes to be approved for CHOSUN operation.

d. (U) Specific identification of proposed compartmented information types to be approved for CHOSUN processing.

e. (U) Any requested waivers with NCWG evaluation and recommendation for approval/disapproval.

4.9 CHOSUN Network Accreditation (U)

(C) The accreditation of the CHOSUN network provides official approval for initial or continued operation of the CHOSUN network, as described in the network certification documents (i.e., specific nodes included, specific compartments, and any operational limitations stated therein). The Assistant to the President for National Security Affairs is the DAA for the CHOSUN network and therefore has the responsibility to issue CHOSUN network accreditation based upon review and evaluation of the accreditation request package forwarded from the NCWG.

(U) As a goal, accreditation of the CHOSUN network will be accomplished within 30 days of forwarding to the DAA the letter of CHOSUN network certification.

(U) Results of network accreditation will be provided immediately to the CHOSUN Network Security Officer to allow prompt initiation of operational activation/re-activation planning.

4.10 Schedule for Recertification and Reaccreditation (U)

(U) Once the CHOSUN network has initially completed requisite certification and accreditation, it will require routine recertification and reaccreditation every twelve months. The Network Security Manual will be reviewed and updated annually as a component activity within the network recertification/reaccreditation process.

(U) In other instances with the potential to necessitate recertification/reaccreditation, the NCWG has the responsibility to analyze the specific situation and develop a recommendation on the need for recertification/reaccreditation. The NCWG may then recommend full network-wide recertification/reaccreditation, or only selected steps of the process. For example, a new node requesting entry to the CHOSUN network may necessitate only certification/accreditation of

the new node and reassessment of system certification based upon the newly provided ST&E rather than recertifying all nodes.

(U) Types of situations which may require network recertification and reaccreditation include:

a. (U) Occurrence of a system/network violation which, in the judgement of the NCWG, requires recertification/reaccreditation.

b. (U) Addition of a new user node.

c. (U) Significant change in the risk environment. This includes the proposed addition of a new compartmented information category and changes in the threat/operating environment.

d. (U) A major change in hardware or software.

In cases of these nonroutine situations with potential for full network recertification/reaccreditation, final responsibility for issuing a call for recertification/reaccreditation lies with the DAA for the CHOSUN network.

4.11 Revoking Accreditation (U)

(U) The DAA may, at any time, revoke the system network accreditation based on any change in the system/network security posture. Types of changes that may cause revocation of accreditation include but are not limited to the following:

a. (U) Occurrence of a system/network violation.

b. (U) A significant change in the risk or threat environment.

c. (U) Information identifying additional system/network vulnerabilities.

(U) The DAA will also be responsible for initiating the recertification/reaccreditation process of the system/network once the change in security posture has been appropriately addressed (see section 4.10).

THIS PAGE INTENTIONALLY LEFT BLANK

SECTION 5. PERSONNEL SECURITY (U)

5.1 General (U)

(U) Installation of the CHOSUN network at multiple nodes in a physically secure area requires stringent entry and access controls to be exercised over all personnel having access to the network and its peripherals. The CHOSUN network will operate in a system-high environment (TS/SCI). Therefore, unescorted access to any CHOSUN facility shall be limited to personnel who are cleared for TOP SECRET and formally approved for access to all special categories of information which will be processed, stored or transmitted by the network and who additionally shall be approved for CHOSUN access by the DAA or NSO.

(U) The granting of access to the CHOSUN operational network shall be controlled under the strictest application of the "need-to-know" principle and in accordance with the personnel security requirements set forth in this document.

5.2 Personnel Identification (U)

(U) Personnel having potential access to CHOSUN network/facilities are identified as users, operators (personnel performing technical functions at the hub and user nodes), and Government and contractor personnel who perform critical support functions in the implementation, testing, and maintenance of the network. Personnel other than those cited above will not be authorized access to the network or node/hub facilities without prior approval of the NSO.

5.3 Access Authorization Process (U)

(U) The process of access authorization to the network or node/hub facilities will be the same for all personnel. The access authorization process will be dependent upon:

a. (U) An access authorization request.

b. (U) Approval of the access authorization request based on:

(1) (U) Determination of need to know, and

(2) (U) Satisfactory background investigation of the individual under consideration for access or evidence of clearance which meets the requirements established by this manual.

5.4 Access Requests (U)

(U) The proper and careful selection of candidates (users or support personnel) for access to CHOSUN is one of the most important facets of CHOSUN security. Effective security is largely dependent upon the personal integrity and security consciousness of the candidate and the nominator. Therefore, emphasis will be placed on the security screening of candidates for CHOSUN access and continued reinforcement of security requirements. Nominators shall ensure that candidates are of the highest quality in terms of loyalty, character, integrity, discretion, and responsibility. Nominations shall be screened for information incompatible with the personnel standards presented in section 5.5 of this manual.

a. (U) Nomination Package Preparation. Nominations for access to Project CHOSUN shall be prepared on the Access Nomination Form provided as appendix G and will include the candidate's full name, rank/grade, Social Security Number, date and place of birth; organization and position assigned; scheduled departure or reassignment, telephone number; security clearance, type of investigation, date granted and by whom; need-to-know justification of access; retention period; certification, by the cognizant security officer, that the individual meets the personal standards set forth in section 5.5, without waiver.

   (1) (U) For those candidates who meet the security clearance criteria set forth in section 5.5, the sponsor (nominator) shall complete the Access Nomination Form and submit it to the NSO for processing.

   (2) (U) For candidates who require a personal security investigation or reinvestigation in order to meet the eligibility requirements, the nominator will submit forms to his cognizant investigative agency for completion of a background investigation that meets the criteria set forth in section 5.5.2.1. Upon completion of the required investigation and determination that the individual meets the prescribed criteria, the justification for the candidate's need-to-know requirement will be forwarded to the NSO.

b. (U) Nomination Package Submission. Nomination packages, including requests for one-time-limited access, shall be submitted by the Program Management Office (PMO), NISSO, or

HISSO to the NSO. The nominator will carefully review the nomination package to determine if the candidate meets the personnel reliability standards and need-to-know requirements before signing the nomination package. Names of individuals not believed by the nominator to meet the need-to-know criteria should not be forwarded to the NSO.

c. (U) Nomination Package Review and Approval. The DAA is the sole authority for authorizing access to potential users of the CHOSUN network. Users are those people who require access to the video/data consoles in support of the national crisis management decisionmaking process. All other personnel seeking access to the node/hub facilities (e.g., maintenance, technical control personnel) will be approved by the NSO.

(U) The adequacy of the justification provided by the nomination for an individual's access to CHOSUN information shall be determined based on the need-to-know criteria. If work can proceed without an individual's knowledge or involvement at the CHOSUN level, then the individual does not meet the criteria.

(U) Approved nomination shall be returned to the nominator, who will arrange for notification of the candidate of the date, time, and place of his security indoctrination briefing and the conduct of the indoctrination (see section 5.6).

5.5 Clearance (U)

(U) Individuals identified as requiring access to the network will meet the following minimum personnel security standards:

a. (U) The individual shall be stable, of excellent character and discretion, and of unquestioned loyalty to the United States.

b. (U) Both the individual and the members of his or her immediate family shall be United States citizens. For these purposes, "immediate family" is defined as including the individual's spouse, parents, brothers, sisters, and children.

c. (U) The members of the individual's immediate family and persons to whom he or she is bound by affection or obligation should neither be subject to physical, mental, or other forms of duress by a foreign power, nor advocate the use of force or violence to overthrow the Government of the

United States or the alteration of the form of Government of the United States by unconstitutional means.

5.5.1 (U) Exceptions. Where there is a compelling need and a determination has been made by the DAA that every reasonable assurance has been obtained and that under the circumstances the security risk is negligible, the standards set forth in sections 5.5.b. or 5.5.c. may be waived. Further, an exception to the provisions of this manual applies for elected officials of the United States Government, Federal judges, and those individuals for whom the DAA makes a specific exception.

5.5.2 (U) Investigative Requirements. The investigation conducted on an individual under consideration for access to CHOSUN will be thorough and shall be designed to develop information as to whether the individual clearly meets the personnel security standards. The investigation will be current within five (5) years prior to an individual's nomination for access to CHOSUN. If the background investigation is over one (1) year old from the date of nomination into CHOSUN, a subject interview and polygraph will be required. Arrangements for polygraph will be made by the agency requesting the access, through the investigative agency which normally provides polygraph support.

(U) The investigation shall be accomplished through record checks and personal interviews of various sources by trained investigative personnel in order to establish positively the complete continuity of identity to include date of birth, residences, education, employment, and military service. Where the circumstances of a case indicate, the investigation shall exceed the basic requirements set forth below to ensure that those responsible for authorizing access have in their possession all the relevant facts in order to determine the candidate's eligibility.

(U) The individual shall furnish a signed personal history statement, fingerprints of a quality acceptable to the investigative agency, and a signed release, as necessary, authorizing custodians of police, credit, education, and medical records, to provide record information to the investigative agency. Photographs of the individual shall also be obtained where additional corroboration of identity is required.

5.5.2.1 (U) Minimum Standards. Minimum standards for the investigation are as follows:

a. (U) Verification of date and place of birth and United States citizenship.

b. (U) Check of the subversive and criminal files of the Federal Bureau of Investigation, including submission of fingerprint charts, and checks of such other national agencies as are appropriate to the individual's background. An additional check of Immigration and Naturalization Service records shall be conducted on those members of the individual's immediate family who are United States citizens other than by birth or who are resident aliens.

c. (U) Check of appropriate police records covering all areas where the individual has resided in the United States throughout the most recent fifteen (15)-year period or since age eighteen, whichever is the shorter period.

d. (U) Verification of the individual's financial status and credit habits through checks of appropriate credit institutions and interviews with knowledgeable sources covering the most recent five (5)-year period.

e. (U) Interviews with neighbors in the vicinity of all the individual's residences in excess of six (6) months throughout the most recent five (5)-year period. This coverage shall be expanded where the investigation suggests the existence of some questionable behavioral pattern.

f. (U) Confirmation of all employment during the past fifteen (15) years or since age eighteen, whichever is the shorter period but in any event the most recent two years. Personal interviews with supervisors and co-workers at places of employment covering the most recent ten (10)-year period.

g. (U) Verification of attendance at all institutions of higher learning and at the last secondary school attended for the most recent fifteen (15)-year period. Attendance at secondary schools may be verified through qualified collateral sources. If attendance at educational institutions occurred within the most recent five (5) years, personal interviews with faculty members or other persons who were acquainted with the individual during his or her attendance will be conducted.

h. (U) Review of appropriate military records.

i. (U) Interviews with a sufficient number of knowledgeable acquaintances (a minimum of three developed during the course of the investigation) as necessary to provide continuity to the extent practicable, of the individual's

activities and behavorial pattern over the past fifteen (15)-years with particular emphasis on the most recent five (5)-years.

j. (U) When employment, education, or residence has occurred overseas (except for periods of less than five (5)-years for personnel on U.S. Government assignment and less than ninety days for other purposes) during the past fifteen (15) years or since age eighteen (whichever is the shorter period), a check of the records will be made at the Department of State and other appropriate agencies. Efforts shall be made to develop sources, generally in the United States, who knew the individual overseas in order to cover significant employment, education or residence and to attempt to determine if any lasting foreign contacts or connections were established during this period. However, in all cases where an individual has worked or lived outside of the United States continuously for over five years, the investigation will be expanded to cover fully this period in his life through the use of such investigative assets and checks of record sources as may be available to the United States Government in the foreign country(ies) in which the individual resided.

k. (U) In those instances in which the individual has immediate family members or other persons with whom he or she is bonded by affection or obligation in any of the situations described in 5.5.c. above, the investigation will include an interview of the individual by trained security, investigative, or counterintelligence personnel to ascertain the facts as they may relate to the individual's access eligibility.

l. (U) In all cases the individual's spouse shall, at a minimum, be checked through the subversive files of the Federal Bureau of Investigation and other appropriate national agencies. When conditions indicate, additional investigation shall be conducted on the spouse of the individual and members of the immediate family to the extent necessary to permit the determination that the personnel security standards presented in this section are met.

m. (U) A personal interview of the individual will be conducted by trained security, investigative or counterintelligency personnel when necessary to resolve any significant adverse information and/or inconsistencies developed during the investigation.

5.5.2.2 (U) Investigative Exceptions. In exceptional cases, the DAA may determine that it is necessary or advisable in the national interest to authorize access prior to completion of the fully prescribed investigation. In this situation, such investigative checks as are immediately possible shall be made at once, and should include a personal interview by trained security or counterintelligence personnel. Access in such cases shall be strictly controlled, and the fully prescribed investigation and final evaluation shall be completed at the earliest practicable time.

5.5.2.3 (U) Special Investigative Requirement. In addition, all personnel identified as operators, Government, and contractor personnel working at the hub will be polygraphed prior to access authorization/approval to the facility.

5.5.2.4 (U) Approved Investigative Agencies. Investigations completed by the following Federal agencies are acceptable if they encompass all of the investigative requirements cited in herein:

a. (U) Central Intelligence Agency.

b. (U) Defense Investigative Service.

c. (U) Department of the Treasury.

d. (U) Federal Bureau of Investigation.

e. (U) Office of Personnel Management.

f. (U) United States Secret Service.

5.6 Security Indoctrination (U)

(U) Once a nomination has been approved, no information or material will be provided to the candidate until he/she has received a security indoctrination briefing and has executed a Non-Disclosure Agreement (NDA). NDAs shall be forwarded to the NSO and controlled by the NSO for a period of 70 years after access termination. Individuals approved for one-time-limited access will also execute both a briefing and debriefing statement at the time of indoctrination.

a. (U) All indoctrinations shall be accomplished by the NSO, PM, NISSO, or HISSO. Indoctrinations shall consist of a general description of the Project, as appropriate, and instructions on how to protect CHOSUN information.

b. (U) Specific instruction shall include the individual's responsibility for notifying the NSO:

(1) (U) Upon any significant change in personal status, (e.g., arrests, convictions, civil lawsuits involving allegations of fraud, deceit or misrepresentation against the individual, change of address, or change of employment).

(2) (U) Upon unauthorized contact with a citizen of a foreign country. (This recognizes the need for certain indoctrinated individuals to undertake activities requiring official contact with foreign nationals).

(3) (U) Upon request for Project CHOSUN information from unauthorized persons.

(4) (U) Upon intent to marry or divorce.

(5) (U) Of the intent to travel to or through any country (countries) listed as denied areas (see DCID 1/20), at least 30 days prior to such travel.

c. (U) Security reindoctrinations shall be conducted annually, or when special events are scheduled to take place (e.g., tests, exercises, and foreign travel).

5.7 Continuing Security Programs (U)

(U) In order to facilitate the attainment of the highest standard of personnel security and to augment both the access approval criteria and the investigative requirements established by this manual, participating CHOSUN departments and agencies shall institute continuing security programs for all individuals having access to CHOSUN. In addition to security indoctrinations, these programs shall be tailored to create mutually supporting procedures under which no issue will escape notice or be left unresolved.

(U) The continuing security programs shall include the following:

a. (U) Security education programs to ensure that individuals who are granted access are initially indoctrinated and periodically thereafter instructed as to its unique sensitivity so that they understand their personal responsibility for its protection. The individual should be instructed that the ultimate responsibility for maintaining eligibility for continued access rests with the individual.

Therefore, the individual is encouraged to seek appropriate guidance and assistance on any personal problem or situation that may have a possible bearing on his eligibility for continued access, and security counseling should be made available. These instructions should be conducted by individuals having extensive background and experience regarding the nature and special vulnerabilities of CHOSUN information.

b. (U) Security supervisory programs to ensure that supervisory personnel recognize and discharge their special responsibility in matters pertaining to the security of CHOSUN information. Such programs shall provide practical guidance as to indicators which may signal matters of security concern. Specific instructions concerning reporting procedures shall be disseminated to enable the appropriate authority to take timely corrective action to safeguard the security of the United States as well as to provide all necessary help to the individual concerned in order to neutralize his vulnerability.

c. (U) Security review programs to ensure that appropriate security authorities receive and exchange, in a timely manner, all information bearing on the security posture of persons having access to sensitive information. Personnel history information shall be kept current. Security and related files shall be kept under continuing review.

d. (U) Periodic reinvestigation (PR) of individuals granted access to CHOSUN information, material, or facilities will be conducted on a five-year recurring basis. The PR shall consist of all pertinent records, etc., enumerated in section 5.5.2.1 above, as applicable for the intervening period.

e. (U) Whenever adverse or derogatory information is discovered or inconsistencies arise that could impact upon an individual's security status, appropriate investigations shall be conducted on a timely basis. The investigation shall be of sufficient scope necessary to resolve the specific adverse or derogatory information, or inconsistency in question so that a determination can be made as to whether the individual's continued participation in activities requiring access to SCI is clearly consistent with the interest of national security.

5.8 Access Termination and Debriefing (U)

(U) Due to the extreme sensitivity of CHOSUN information and locations, access must be limited to those persons requiring access for the performance of their duties.

a. (U) Individuals no longer requiring access to CHOSUN information or who may be terminated for cause shall be debriefed by the PMO, NISSO, or HISSO and removed from the CHOSUN access roster by the NSO. As part of the debriefing process, departing individuals must complete a Security Termination Statement that will be forwarded to the NSO for retention.

b. (U) Access by individuals authorized for one-time-limited access shall automatically terminate at the end of the access period.

c. (U) For those individuals having access to the operational network, the NSO will be responsible for deleting each departing individual's USERID/password from the system and rescinding the previously approved access authorization. The NISSO will delete each departing individual's USERID/password from the node's word processor.

SECTION 6. PHYSICAL SECURITY (U)

6.1 General (U)

(U) The extreme sensitivity of the CHOSUN network requires extraordinary physical security measures to guard against unauthorized access to the nodes, hub, or any other component of the CHOSUN facility. The standards set forth in this manual will be adhered to at all times, whether the specific node is operational or inactive.

6.2 Structural Barriers (U)

(U) Requirements for parent rooms are outlined below:*

a. (U) Parent room walls will be constructed from truefloor to trueceiling, with all openings in excess of 90 square inches barred, baffled, and alarmed to detect any attempted intrusion of personnel or listening/eavesdropping/transmitting devices. Standard wall construction, consisting of drywall with either metal or wooden studs, will be considered adequate. Expanded steel (9-11 gauge) and three (3) inches of fiberglass insulation are required in addition to standard wall construction on all facilities (e.g., conference rooms) which do not have RF shields.

(1) (U) Parent Room Housing an RF-Shielded Room. Maintain a minimum of 18 inches of "dead space" between the exterior of the RF-shielded room and the interior of the parent room perimeter walls.

(2) (U) Parent Room Housing RF-Shielded Cabinet/Racks. Provide a minimum of STC 45 when measured at the exterior of the parent room walls.

b. (U) Exterior doors will be constructed of 1 3/4-inch-solid material, with hinge pins bradded or welded to preclude removal. Each exterior door will have a three (3)-position, changeable combination; GSA-approved, Group 1 lock; acoustic seal; and pneumatic door closer. Combinations will be changed by CHOSUN-approved individuals only, at least every six (6) months, recorded on the appropriate form, and forwarded to the NSO for storage. Local storage of combinations is not authorized.

*(U) A parent room is defined as the space located inside a building structure, within which is assembled either an RF-shielded enclosure or one or more RF-shielded cabinet/racks.

6.3 Intrusion Detection Systems (U)

6.3.1 (U) Perimeter Intrusion Detection. CHOSUN facilities will be provided with perimeter intrusion detection systems to include, but not be limited to:

a. (U) Balanced magnetic switches on all exterior doors, configured for day/night use.

b. (U) Vibration detection of the interior of all perimeter walls, active 24 hours a day.

c. (U) Passive infrared or omnidirectional ultrasonic detection between the exterior wall and the RF shield, active 24 hours a day.

d. (U) Line supervision between the facility and the annunciator panel where the alarm is monitored, which will sound an alarm in case of system failure or tampering.

e. (U) If the facility will not be continuously staffed 24 hours a day, 7 days a week, passive infrared detection will be installed within the RF shield.

f. (U) All alarm sensors and control boxes will have tamper-proof switches.

g. (U) All alarm systems will have 8-12-hour battery standby power.

h. (U) All control boxes will be located inside the alarmed area.

6.3.2 Monitoring and Alarm Response (U)

a. (U) A central station alarm monitoring system for each node must be installed or integrated into existing alarm consoles which will annunciate any alarm condition which occurs at the CHOSUN facility. Zones must be configured in such a way as to indicate the location of the alarm at the facility (e.g., front door, "dead space" between RF shield and outer wall of the parent room). Attempted entries with an invalid card-reader card or individual identifier number should also cause an alarm condition to occur.

b. (U) The central station will be staffed 24 hours a day, 7 days a week, and may not be left unattended for even short periods of time.

c. (U) Responses to alarms will be immediate and occur in all cases of an alarm condition. Response time will not exceed 5 minutes. Only appropriately trained security personnel should be designated to respond to alarms.

6.3.3 Emergency Conditions (U)

a. (U) The facility shall be equipped with HALON or a similar fire suppressant.

b. The CHOSUN facility should be staffed by a minimum of two people at all times both for security considerations and safety considerations (e.g., in the event one person is incapacitated due to medical emergency or fire).

c. (U) All facilities will have water detectors that trigger an alarm in case of flooding. Plastic tarpaulins will be available to cover equipment in case of pipe breakage.

d. (U) The physical security features of CHOSUN facilities are such that they would preclude rapid response into the facility unless the doors are opened from the inside.

e. (U) In a medical emergency or fire, preservation of life is of paramount importance. Access will be granted to doctors, emergency medical teams, and firefighters as necessary. If practical, the system will be shut down and classified material will be secured or covered prior to allowing access. This should not, however, delay entrance.

f. (U) If possible, a CHOSUN-approved individual should be present within the facility as long as it does not create a hazard to the individual. Extraneous and/or unnecessary personnel should not be allowed into the area.

g. (U) All facilities (nodes and hub) will be equipped with an interruptible power supply.

6.4 Access Control (U)

6.4.1 (U) Access Roster. A roster of personnel approved for and authorized access to CHOSUN facilities will be maintained by the NSO and transmitted via the CHOSUN network to all nodes on a weekly basis. Each node will receive only the listing of individual's approved for access to that node. This roster will contain the name, Social Security Number, date of birth, place of birth, level of clearance, agency, nodes to which the individual has been approved for access, and date of approval.

6.4.1.1 (U) Access by Uncleared Service Personnel. Uncleared service personnel (e.g., electricians, carpenters, plumbers, construction, cleaning, and delivery personnel) will be provided a one-for-one escort at all times while in the CHOSUN facility.

6.4.1.2 (U) Access by Emergency Personnel. Access by emergency personnel shall be in accordance with the provisions of paragraph 6.3.3.d. above.

6.4.2 (U) Intra-Agency Access. Intra-agency access to a CHOSUN facility will be controlled by a card-reader access control which requires both a valid, electronically read card and three-number, unique identifier code to be entered separately by the individual. The NSO will change identifier codes at least semi-annually and maintain a record of the change for one (1) year. Card-reader systems will be installed with an Uninterruptible Power Supply (UPS) or have a backup system which will sustain complete operation for a minimum of eight (8) hours. The system must also be capable of allowing egress while denying ingress in case of a system failure. The card-reader system must not be installed on the door of the RF-shielded rooms but must be installed on the door of the parent room.

6.4.3 (U) Inter-Agency Access. The access roster distributed by the NSO will be the basis for determining if an individual authorized CHOSUN facility access at one node will be automatically allowed access to a CHOSUN facility at another node. If the visitor is approved for CHOSUN access at one node but not at the node being visited, access to the visited node may be granted at the discretion of the visited agency.

6.4.4 (U) Non-Approved Personnel Access. Access by non-CHOSUN-approved personnel will be held to an absolute minimum, consistent with operational needs of the CHOSUN network, and under the constraints indicated below. A record of such visits will be made and maintained for one (1) year. This record will include the name, organization, date, time entered, time departed, purpose of visit, and signature of escort. Each node shall coordinate with the Network Security Officer prior to granting access to non-CHOSUN-approved personnel.

(U) Each CHOSUN facility will have red flashing lights installed in the ceiling of the facility in sufficient quantities to ensure that they are visible to all personnel working within the facility. Prior to entry of non-CHOSUN-approved personnel into the facility, these red lights will be activated to inform all personnel that a non-approved person is present and the node will be disconnected from the network. The visitor will be under constant escort by a CHOSUN-approved individual. Badges will be issued to non-CHOSUN-approved individuals. These badges must conspicuously indicate that the individual is non-CHOSUN approved. These badges must be worn on

an exterior garment, above waist level.

6.4.5 (U) Badges. Control and issuance of badges and identification numbers are the responsibility of each node; however, certain procedures must be followed in order to ensure the integrity of the access control system. These procedures include the following:

a. (U) All issued badges will be accounted for by receipt to include the signature of the individual who has been issued the badge.

b. (U) All unissued badges will be stored in a separate locked container within the CHOSUN facility. Unissued badges will be inventoried monthly.

c. (U) All individual identifier codes must be randomly computer generated, from within the CHOSUN facility.

d. (U) All individual identifier codes which have been issued will be listed in a roster separate from the badge issuance receipt system and sealed in a double envelope within the container where blank badges are maintained.

e. (U) The central processing unit of the card-reader system will be stored within the CHOSUN facility and locked in a manner to preclude tampering.

f. (U) All lost or stolen badges will be immediately reported to the issuing authority. The issuing authority will void both the badge and identification number from the system.

g. (U) An event recorder will be connected to the central processing unit of the card reader system which will record all entrances, exits, invalid attempts, and alarm conditions. A copy of these records will be maintained for a period of thirty (30) days.

h. (U) Card-reader badges for access to a CHOSUN facility should not leave the building in which the facility is located. A system must be developed by each agency whereby agency identification cards, building access, or other similar identification is exchanged for the card-reader badge. This exchange must, of course, occur outside the CHOSUN facility, and adequate security must be provided to this area to preclude loss or theft. (Agencies may propose alternate methods of access control which provide the same level of security (e.g., two-person reception area with access roster and individual picture identification). The DAA will approve all alternate methods via a Request for Waiver.)

6.5 Equipment Delivery (U)

(U) Security problems are increased when property and material are in transit. Loading and unloading procedures, compartmentalization of cargoes in ships, railroad cars, aircraft, and movements of such carriers present security hazards of varying degrees. It is recommended that all electronic equipment and supplies be delivered as directly as possible from the source to a neutral address at the user agency and that the deliveries be accompanied by a qualified security officer.

(U) To provide for the security of property and material in transit, the responsibilities of the consignor, the carrier, and the consignee must be clearly established. The protection of such property and material is, in general, the responsibility of the person who has the property in his custody. It is the responsibility of the consignor to ensure that all cargo requiring security protection is entrusted only to carriers properly cleared for handling this cargo.*

*(U) A more stringent OPSEC requirement needs to be developed for the delivery of technical and nontechnical equipment (e.g., furniture).

SECTION 7. INFORMATION SECURITY (U)

(C) The dissemination of Project CHOSUN information must be stringently controlled to protect crisis management at the national level. Appendix C, the CHOSUN Security Classification Guide provides basic guidance for determining (1) the security classification of CHOSUN information, and (2) schedules for downgrading or declassifying information. The guide is designed to protect sensitive information regarding the architecture, design, capabilities, and limitations of Project CHOSUN from adversaries.

(C) Project CHOSUN related information is the property of The National Security Council in the Executive Office of the President of the United States. Any release of this information, either classified or unclassified, to persons outside The Executive Branch must be approved in writing by the NSO. All documents related to Project CHOSUN will be marked "Property of The National Security Council. Written Approval Required for Release."

(U) The information provided in this section is extracted from DOD 5200.1-R, Information Security Program Regulation. It provides detailed procedures for the marking, control, and accountability of classified information.

7.1 Marking (General Provisions) (U)

(U) Information determined to require classification protection under this manual shall be so designated. Designation by means other than physical marking may be used but shall be followed by physical marking as soon as possible. Designation by physical marking, notation, or other means serves (1) to warn the holder about the classification of the information involved, (2) to indicate the degree of protection against unauthorized disclosure that is required for that particular level of classification, and (3) to facilitate downgrading and declassification actions.

7.1.1 (U) Original Classification. At the time of original classification, the following shall be shown on the face of all originally classified documents or clearly associated with other forms of classified information in a manner appropriate to the medium involved:

a. (U) The identity of the original classification authority by position title, unless he or she is the signer or approver of the documents.

b. (U) The agency and office of origin.

c. (U) The overall classification of the document.

d. (U) The date or event for automatic declassification or notation "Originating Agency's Determination Required" or "OADR."

e. (U) Any downgrading action to be taken and the date or event thereof.

7.1.2 (U) Derivative Classification. At the time of derivative classification, the following shall be shown on the face of all derivatively classified documents or clearly associated with other forms of classified information in a manner appropriate to the medium involved:

a. (U) The source of classification; that is, the source document or classification guide. If classification is derived from more than one source, the phrase "Multiple Sources" will be shown and the identification of each source will be maintained with the file or record copy of the document.

b. (U) The agency and office of the derivatively classified document.

c. (U) The overall classification of the document.

d. (U) The date or event for declassification or the notation "Originating Agency's Determination Required" or "OADR," carried forward from the classification source. If the classification is derived from multiple sources, either the most remote date or event for declassification marked on the sources or if required by any source, the notation "Originating Agency's Determination Required" or "OADR" shall be shown.

e. (U) Any downgrading action to be taken and the date or event thereof.

7.1.3 (U) Identification of Classification Authority. Identification of a classification authority shall be shown on the "Classified by" line and shall be sufficient, standing alone, to identify a particular official, source document or classification guide.

(U) If any information in a document or material is classified as an act of original classification, the classification authority who made the determination shall be identified on the "Classified by" line unless the classifier is also the signer or approver of the document.

(U) If the classification of all information in a document or material is derived from a single source (for example, a source document or classification guide), the "Classified by" line shall identify the source document or classification guide, including its date when necessary to ensure positive identification.

(U) If the classification of information contained in a document or material is derived from more than one source document, classification guide, or combination thereof, the "Classified by" line shall be marked "Multiple Sources" and identification of all such sources shall be maintained with the file or record copy of the document.

(U) If an official with requisite classification authority has been designated by the head of an activity to approve security classification assigned to all information leaving the activity, the title of that designated official shall be shown on the "Classified by" line. The designated official shall maintain records adequate to support derivative classification actions.

7.1.4 (U) Declassification and Regrading Procedures. Whenever classified information is downgraded or declassified earlier than originally scheduled, or upgraded, the material shall be marked promptly and conspicuously to indicate the change, the authority for the action, the date of the action, and the identity of the person taking the action. In addition, except for upgrading, prior classification markings shall be cancelled, if practicable, but in any event those on the first page, and the new classification markings, if any, shall be substituted. When classified information is downgraded or declassified in accordance with the assigned downgrading and declassification markings, such markings shall be a sufficient notation of the authority for such action.

7.1.5 (U) Applying Derivative Declassification Dates. New material that derives its classification from information classified on or after August 1, 1982, shall be marked with the declassification date, event, or the notation "Originating Agency's Determination Required" or "OADR" assigned to the source information.

(U) New material that derives its classification from information classified prior to August 1, 1982, shall be treated as follows:

a. (U) If the source material bears a declassification date or event, that date or event shall be carried forward to the new material.

b. (U) If the source material bears no declassification date or event or bears an indeterminate date or event such as "Upon Notification by Originator," "Cannot be Determined,"

or "Impossible to Determine," or is marked for declassification review, the new material shall be marked with the notation "Originating Agency's Determination Required" or "OADR."

c. (U) If the source material is foreign Government information bearing no date or event for declassification or is marked for declassification review, the new material shall be marked with the notation "Originating Agency's Determination Required" or "OADR."

(U) New material that derives its classification from a classification guide issued prior to August 1, 1982, that has not been updated to conform with this Regulation shall be treated as follows:

a. (U) If the guide specifies a declassification date or event, that date or event shall be applied to the new material.

b. (U) If the guide specifies a declassification review date, the notation "Originating Agency's Determination Required" or "OADR" shall be applied to the new material.

7.1.6 (U) Upgrading. When material is upgraded, it shall be promptly and conspicuously marked as prescribed, except that in all such cases the old classification markings shall be cancelled and new markings substituted.

7.1.7 (U) Dissemination and Reproduction Notice. Classified information that the originator has determined to be subject to special dissemination or reproduction limitations, or both, shall include, as applicable, a statement or statements on its cover sheet, first page or in the text, substantially as follows:

"Reproduction requires approval of originator. Further dissemination only as directed by (Insert appropriate office or official)."

7.2 Marking Documents (U)

7.2.1 (U) Overall and Page Marking. Except as otherwise specified for working papers, the overall classification of a document, whether or not permanently bound, or any copy or reproduction thereof, shall be conspicously marked, stamped or affixed permanently at the top and bottom on the outside of the front cover (if any), on the title page (if any), on the first page, and on the outside of the back cover (if any). Each interior page shall be marked top and bottom according to its content. Alternatively, the overall classi-

fication of the document may be conspicuously marked or stamped at the top and bottom of each interior page when such marking is necessary to achieve production efficiency and the particular information to which classification is assigned is otherwise sufficiently identified. In any case, the classification marking of a page shall not supersede the classification marking of portions of the page marked with lower levels of classification.

7.2.2 (U) Marking Components. The major components of some complex documents are likely to be used separately. In such instances, each major component shall be marked as a separate document. Examples include each annex, appendix, or similar component of a plan, program or operations order; attachments and appendices to a memorandum or letter; each major part of a report.

7.2.3 (U) Portion Marking. Each section, part, paragraph, or similar portion of a classified document shall be marked to show the level of classification of the information contained in or revealed by it, or that it is unclassified. Portions of documents shall be marked in a manner that eliminates doubt as to which of its portions contains or reveals classified information. Classification levels of portions of a document shall be shown by the appropriate classification symbol placed immediately following the portion's letter or number, or in the absence of letters or numbers, immediately before the beginning of the portion. In marking sections, parts, paragraphs, or similar portions the parenthetical symbols "(TS)" for TOP SECRET, "(S)" for SECRET, "(C)" for CONFIDENTIAL, and "(U)" for UNCLASSIFIED, shall be used. When appropriate, the symbols "RD" for Restricted Data and "FRD" for Formerly Restricted Data shall be added, for example, "(S-RD)" or "(C-FRD)." In addition, portions that contain Critical Nuclear Weapon Design Information (CNWDI) will be marked "(N)" following the classification, for example, "(S-RD) (N)."

(U) Illustrations, photographs, figures, graphs, drawings, charts, and similar portions of classified documents will be clearly marked to show their classification or unclassified status. Such markings shall not be abbreviated and shall be prominent and placed within or contiguous to the portion. Captions of such portions shall be marked on the basis of their content also by placing the symbol "(TS)," "(S)," "(C)," or "(U)" immediately preceding the caption.

(U) If, in an exceptional situation, parenthetical portion marking is determined to be impracticable, the document shall contain a statement sufficient to identify the information that is classified and the level of such classification. Thus, for example, each portion of a classified document need not be separately marked if all portions are classified at the same level, provided a statement to that effect is included in the document.

(U) When elements of information in one portion require different classifications, but segregation into separate portions would destroy continuity or context, the highest classification required for any item shall be applied to that portion or paragraph.

7.2.4 (U) Compilations. When classification is required to protect a compilation of information, the overall classification assigned to such documents shall be placed conspicuously at the top and bottom of each page and on the outside of the front and back covers, if any, and an explanation of the basis for the assigned classification shall be included on the document or in its text.

7.2.5 (U) Subjects and Titles of Documents. Subjects and titles of classified documents shall be marked with the appropriate symbol, "(TS)," "(S)," "(C)," or "(U)" placed immediately following and to the right of the item. When applicable, other appropriate symbols, for example, "(RD)" or "(FRD)" shall be added.

7.2.6 (U) File, Folder, or Group of Documents. When a file, folder, or group of classified documents is removed from secure storage, it shall be marked conspicuously with the highest classification of any classified document included therein or shall have an appropriate classified document cover sheet affixed.

7.2.7 (U) Transmittal Document. A transmittal document, including endorsements and comments when such endorsements and comments are added to the basic communications, shall carry on its face a prominent notation of the highest classification of the information transmitted by it, and a legend showing the classification, if any, of the transmittal document, endorsement, or comment standing alone. For example, an unclassified document that transmits as an attachment a classified document shall bear a notation substantially as follows: "UNCLASSIFED WHEN SEPARATED FROM CLASSIFIED ENCLOSURE."

7.3 Marking Classified Information Other Than Documents (U)

(U) Security classification and applicable associated markings assigned by the classifier shall be conspicuously stamped, printed, written, painted, or affixed by means of a tag, sticker, decal, or similar device, on classified material other than paper copies of documents, and on containers of such material, if possible. If marking the material or container is not practicable, written notification of the security classification and applicable associated markings shall be furnished to recipients. The following procedures for marking various kinds of material containing classified information are not all inclusive and may be varied to accommodate the physical characteristics of the material containing the classified information and to accommodate organizational and operational requirements.

7.3.1 (U) Charts, Maps, and Drawings. Charts, maps and drawings shall bear the appropriate classification marking for the legend, title, or scale blocks in a manner that differentiates between the overall classification of the document and the classification of the legend or title itself. The higher of these markings shall be inscribed at the top and bottom of each such document. When folding or rolling charts, maps, or drawings would cover the classification markings, additional markings shall be applied that are clearly visible when the document is folded or rolled. Applicable associated markings shall be included in or near the legend, title, or scale blocks.

7.3.2 (U) Photographs, Films, and Recordings. Photographs, films (including negatives), recordings, and their containers shall be marked to assure that a recipient or viewer will know that classified information of a specific level of classification is involved.

a. (U) Photographs. Negatives and positives shall be marked, whenever practicable, with the appropriate classification designation and applicable associated markings. Roll negatives or positives may be so marked at the beginning and end of each strip. Negatives and positives shall be kept in containers bearing conspicuous classification markings. All prints and reproductions shall be conspicuously marked with the appropriate classification designation and applicable associated markings on the face side of the print if possible. When such markings cannot be applied to the face side, they may be stamped on the reverse side or affixed by pressure tape label, stapled strip, or other comparable means. (NOTE: When self-processing film or paper is used to photograph or reproduce classified information, all parts of the last exposure shall be removed from the camera and destroyed as classified waste, or the camera shall be protected as classified).

b. (U) Transparencies and Slides. Applicable classification markings shall be shown clearly on the image of each transparency or slide, if possible, or on its border, holder, or frame. Other applicable associated markings shall be shown on the border, holder, or frame.

c. (U) Motion Picture Films. Classified motion picture films and video tapes shall be marked at the beginning and end of each reel by titles bearing the appropriate classification and applicable associated markings. Such markings shall be visible when projected. Reels shall be kept in containers bearing conspicuous classification and applicable associated markings.

bearing conspicuous classification and applicable associated markings.

d. (U) Recordings. Sound, magnetic, or electronic recordings shall contain at the beginning and end a clear statement of the assigned classification that will provide adequate assurance that any listener or viewer will know that classified information of a specified level is involved. Recordings shall be kept in containers or on reels that bear conspicuous classification and applicable associated markings.

e. (U) Microforms. Microforms are images, usually produced photographically on transparent or opaque materials, in sizes too small to be read by the unaided eye. Accordingly, the assigned security classification and abbreviated applicable associated markings shall be conspicuously marked on the microform medium or its container, so as to be readable by the unaided eye. These markings shall also be included on the image so that when the image is enlarged and displayed or printed, the markings will be conspicuous and readable. Such marking will be accomplished as appropriate for the particular microform involved. For example, roll film microforms (or roll microfilm employing 16, 35, 70, or 105 mm films) may generally be marked as provided for roll motion picture film.

7.3.3 (U) Decks of ADP Punched Cards. When a deck of classified ADP punched cards is handled and controlled as a single document, only the first and last card require classification markings. An additional card shall be added (or the job control card modified) to identify the contents of the deck and the highest classification therein. Such additional cards shall include applicable associated markings. Cards removed for separate processing or use and not immediately returned to the deck shall be protected to prevent compromise of any classified information contained therein, and for this purpose shall be marked individually.

7.3.4 (U) Removable ADP and Word Processing Storage Media.

a. (U) External. Removable information storage media on devices, used with ADP systems and typewriters or word processing systems, shall bear external markings clearly indicating the classification of the information and applicable associated markings. Include are media and devices that store information recorded in analog or digital form and that are generally mounted or removed by the users or operators. Examples include magnetic tape

b. (U) Internal. ADP systems and word processing systems employing such media shall provide for internal classification marking to assure that classified information contained therein that is reproduced or generated, will bear applicable classification and associated markings. An exception may be made by the agency head, or designee, for the purpose of exempting existing word processing systems when the internal classification and applicable associated markings cannot be implemented without extensive system modification, provided procedures are established to ensure that users and recipients of the media, or the information therein, are clearly advised of the applicable classification and associated markings.

7.3.5 (U) Documents Produced by ADP Equipment. At a minimum, the first page, and the front and back covers, if any, of documents produced by ADP equipment shall be marked. Classification markings of interior pages may be applied by the ADP equipment or by other means. When the application of associated markings by the ADP equipment is not consistent with economical and efficient use of such equipment, such markings may be applied to a document produced by ADP equipment by superimposing upon the first page of such document a "Notice of Declassificaion Instructions and Other Associated Markings." Such notice shall include the date or event for declassification or the notation "Originating Agency's Determination Required" or "OADR" and all other such applicable markings. If individual pages of a document produced by ADP equipment are removed or reproduced for distribution to other users, each such page or group of pages shall be marked as prescribed, or by superimposing on each such page or group of pages, a copy of any "Notice of Declassification Instructions and Other Associated Markings" applicable to such page or group of pages.

7.3.6 (U) Material for Training Purposes. In using unclassified documents or material to simulate classified documents or material for training purpose, such documents or material shall be marked clearly to indicate the actual unclassified status of the information, for example, "(insert classification designation) for training, otherwise "unclassified" or "UNCLASSIFIED SAMPLE."

7.3.7 (U) Miscellaneous Material. Documents and material such as rejected copy, typewriter ribbon, carbons, and similar items developed in connection with the handling, processing, production, and use of classified information shall be handled in a manner that assures adequate protection of the classified information involved and destruction at the earliest practicable time. Unless a requirement exists

to retain this material or documents for a specific purpose, there is no need to mark, stamp, or otherwise indicate that the information is classified.

7.4 Additional Markings (U)

(U) The warning notices prescribed in this section shall be prominently displayed on classified documents or materials, when applicable. In the case of documents, these warning notices shall be marked conspicuously on the outside of the front cover, or on the first page if there is not a front cover. Transmittal documents, including those that are unclassified shall also bear these additional warning notices, when applicable.

(U) When display of warning notices on other materials is not possible, their applicability to the information shall be included in the written notification of the assigned classification.

7.4.1 (U) Wholly UNCLASSIFIED Material. Normally, unclassified material shall not be marked or stamped "UNCLASSIFIED" unless it is essential to convey to a recipient of such material that it has been examined with a view to imposing a security classification and that it has been determined that it does not require classification.

7.4.2 (U) Restricted Data. Classified documents or material containing Restricted Data as defined in the Atomic Energy Act of 1954, as amended, shall be marked as follows:

"RESTRICTED DATA"

"This material contains Restricted Data as defined in the Atomic Energy Act of 1954. Unauthorized disclosure subject to administrative and criminal sanctions."

7.4.3 (U) Formerly Restricted Data. Classified documents or material containing Formerly Restricted Data, as defined in section 142.d, Atomic Energy Act of 1954, as amended, but no Restricted Data, shall be marked as follows:

"FORMERLY RESTRICTED DATA"

"Unauthorized disclosure subject to administrative and criminal sanctions. Handle as Restricted Data in foreign dissemination. Section 144.b, Atomic Energy Act, 1954."

7.4.4 (U) Special Access Program Documents and Material. Additional markings as prescribed in directives, regulations, and instructions relating to an approved Special Access Program shall be applied to

relating to an approved Special Access Program shall be applied to documents and material containing information subject to the special access program. Such additional markings shall not serve as the sole basis for continuing classificaion of the documents or material to which the markings have been applied. When appropriate, such markings shall be excised to ease timely declassification, downgrading, or removal of the information from special control procedures.

7.4.5 (U) Intelligence Sources and Methods Information. Documents that contain information relating to intelligence sources or methods shall include the following marking:

"WARNING NOTICE--Intelligence Sources
or Methods Involved"

7.4.6 (U) COMSEC Material. Before release to contractors, a COMSEC document will indicate on the title page, or first page if no title page exists, the following notation:

"COMSEC Material - Access by Contractor Personnel Restricted to U.S. Citizens Holding Final Government Clearance."

This notation shall be placed on COMSEC documents or material when originated and when release to contractors can be anticipated. Other COMSEC documents or material shall be marked in accordance with National COMSEC Instruction (NACSI) 4005. Foreign dissemination of COMSEC information is governed by NCSC Policy Directive 14-2.

7.4.7 (U) Associated Markings. Other applicable associated markings required for documents shall be accomplished as prescribed in this section or in any other appropriate manner.

7.5 Storage and Safekeeping (U)

7.5.1 (U) General. Classified information shall be stored only under conditions adequate to prevent unauthorized persons from gaining access. The requirements specified in this manual represent the minimum acceptable security standards.

7.5.2 (U) Standards for Storage Equipment. The GSA establishes and publishes minimum standards, specifications, and supply schedules for containers, vaults, alarm systems, and associated security devices suitable for the storage and protection of classified information. Heads of agencies may establish additional controls to prevent unauthorized access. Security filing cabinets conforming to Federal specifications bear a Test Certification Label on the locking drawer, attesting to the security capabilities of the

container and lock. (On some older cabinets the label was affixed on the inside of the locked drawer compartment.) Cabinets manufactured after February 1962 indicate "General Services Administration Approved Security Container" on the outside of the top drawer.

7.5.3 (U) Storage of Classified Information. Classified information that is not under the personal control and observation of an authorized person will be guarded or stored in a locked security container as prescribed below:

a. (U) TOP SECRET. TOP SECRET information shall be stored in:

(1) (U) A safe-type steel file container having a built-in three-position, dial-type combination lock approved by the GSA or a Class A vault or vault-type room that meets the standards established by the head of the agency concerned. When located in buildings, structural enclosures, or other areas not under U.S. Government control, the storage container, vault, or vault-type room must be protected by an alarm system or guarded during nonoperating hours.

(2) (U) An alarmed area, provided such facilities are adjudged by the local responsible official, to afford protection equal to or better than that prescribed in a. (1) above. When an alarmed area is used for the storage of TOP SECRET material, the physical barrier must be adequate to prevent (1) surreptitious removal of the material, and (2) observation that would result in the compromise of the material. The physical barrier must be such that forcible attack will give evidence of attempted entry into the area. The alarm system must provide immediate notice to a security force of attempted entry. Under field conditions, the field commander will prescribe the measures deemed adequate to meet the storage standards contained in a. (1) and (2) above.

b. (U) SECRET and CONFIDENTIAL. SECRET and CONFIDENTIAL information shall be stored in the manner prescribed for TOP SECRET; or in a Class B vault, or a vault-type room, strong room, or secure storage room that meets the standards prescribed by the head of the agency.

7.5.4 (U) Designations and Combinations.

a. (U) Numbering and Designating Storage Facilities. There shall be no external mark as to the level of classified information authorized to be stored therein. For identification purposes each vault or container shall bear externally an assigned number or symbol.

b. (U) Combination to Containers.

(1) (U) Changing. Combinations to security containers shall be changed only by individuals having that responsibility and an appropriate security clearance. Combinations shall be changed:

(a) (U) When placed in use.

(b) (U) Whenever an individual knowing the combination no longer requires access.

(c) (U) When the combination has been subject to possible compromise.

(d) (U) At least semiannually.

(e) (U) When taken out of service.

(U) Built-in combination locks shall be reset to the standard combination 50-25-50; combination padlocks shall be reset to the standard combination 10-20-30.

(2) (U) Classifying Combinations. The combination of a vault or container used for the storage of classified information shall be assigned a security classification equal to the highest category of the classified information authorized to be stored therein.

(3) (U) Recording Storage Facility Data. A record shall be maintained for each vault, secure room or container used for storing classified information, showing location of the container, the names, home addresses, and home telephone numbers of the individuals having knowledge of the combination.

(4) (U) Dissemination. Access to the combination of a vault or container used for the storage of classified information shall be granted only to those individuals who are authorized access to the classified information stored therein.

c. (U) Electrically Actuated Locks. Electrically actuated locks (for example, cypher and magnetic strip card locks) do not afford the required degree of protection of classified information.

7.6 Accountability and Control (U)

7.6.1 (U) Procedures for Handling TOP SECRET Information. Agencies shall establish the following procedures for handling TOP SECRET information.

7.6.1.1 (U) Control. TOP SECRET Control Officers and alternates shall be designated within offices to be responsible for receiving, dispatching, and maintaining an accountability register of TOP SECRET documents. Such individuals shall be selected on the basis of experience and reliability, and shall have appropriate security clearances.

7.6.1.2 (U) Accountability

a. (U) TOP SECRET Registers. TOP SECRET accountability registers shall be maintained by each office originating or receiving TOP SECRET information. Such registers shall be retained for 5 years and shall, as a minimum, reflect the following:

(1) (U) Sufficient information to identify adequately the TOP SECRET document or material to include the title or appropriate short title, date of the document, and identification of the originator.

(2) (U) The date the document or material was received.

(3) (U) The number of copies received or later reproduced.

(4) (U) The disposition of the TOP SECRET document or material and all copies of such documents or material.

b. (U) Serialization. Copies of TOP SECRET documents and material shall be numbered serially.

c. (U) Disclosure Records. Each TOP SECRET document or item of material shall have appended to it a TOP SECRET disclosure record. The name and title of all individuals, including stenographic and clerical personnel to whom information in such documents and materials has been disclosed, and the date of such disclosure, shall be recorded thereon. Disclosures to individuals who may have had access to containers

in which TOP SECRET information is stored, or who regularly handle a large volume of such information need to be so recorded. Such individuals, when identified on a roster, are deemed to have had access to such information. Disclosure records shall be retained for 2 years after the documents or materials are transferred, downgraded, or destroyed.

d. (U) Inventories. All TOP SECRET documents and material shall be inventoried at least once annually. The inventory shall reconcile the TOP SECRET accountability register with the documents or material on hand. At such times, each document or material shall be examined for completeness. Agency officials may authorize the annual inventory of TOP SECRET documents and material in repositories, libraries, or activities that store large volumes of TOP SECRET documents or material to be limited to documents and material to which access has been granted within the past year, and 10 percent of the remaining inventory.

e. (U) Retention. TOP SECRET information shall be retained only to the extent necessary to satisfy current requirements. Custodians shall destroy nonrecord copies of TOP SECRET documents when no longer needed. Record copies of documents that cannot be destroyed shall be reevaluated and, when appropriate, downgraded, declassified, or retired to designated records centers.

f. (U) Receipts. TOP SECRET documents and material will be accounted for by a continuous chain of receipts.

7.6.2 (U) Procedures for Handling SECRET Information. Administrative procedures shall be established controlling SECRET material originated or received by an activity; distributed or routed to a sub-element of such activity; and disposed of by the activity by transfer of custody or destruction. The control system for SECRET must be determined by the practical balance of security and operating efficiency.

7.6.3 (U) Procedures for Handling CONFIDENTIAL Information. Administrative controls shall be established to protect CONFIDENTIAL information received, originated, transmitted, or stored by an activity.

7.6.4 (U) Procedures for Handling Working Papers. Working papers are documents and material accumulated or created in the preparation of finished documents and material. Working papers containing classified information shall be:

a. (U) Dated when created.

b. (U) Marked with the highest classification of any information contained therein.

c. (U) Protected in accordance with the assigned classification.

d. (U) Destroyed when no longer needed.

e. (U) Accounted for, controlled, and marked in the manner prescribed for a finished document of the same classification when any of the following occurs:

(1) (U) Released by the originator outside the activity or transmitted electrically or through message center channels within the activity.

(2) (U) Retained more than 90 days from date of origin.

(3) (U) Filed permanently.

(4) (U) TOP SECRET information contained therein.

7.6.5 (U) Receipt of Classified Material. Procedures shall be developed within agencies to protect incoming mail, bulk shipments, and items delivered by messenger until a determination is made whether classified information is contained therein. Screening points shall be established to limit access to classified information to cleared personnel.

7.6.6 (U) Restraint on Reproduction. Portions of documents and materials that contain TOP SECRET information shall not be reproduced without the consent of the originator or higher authority. Any stated prohibition against reproduction shall be strictly observed. The following measures apply to reproduction equipment and to the reproduction of classified information.

a. (U) Copying of documents containing classified information shall be minimized.

b. (U) Officials authorized to approve the reproduction of TOP SECRET information shall be designated by position title and shall review the need for reproduction of classified documents and material with a view toward minimizing reproduction.

c. (U) Specific reproduction equipment shall be designated for the reproduction of classified information. Rules for reproduction of classified information shall be posted on or near the designated equipment.

d. (U) Notices prohibiting reproduction of classified information shall be posted on equipment used only for the reproduction of unclassified information.

e. (U) Agencies shall ensure that the equipment used for reproduction of classified information does not leave latent images in the equipment or on other material.

f. (U) All copies of classified documents reproduced for any purpose, including those incorporated in a working paper, are subject to the same controls prescribed for the document from which the reproduction is made.

g. (U) Records shall be maintained to show the number and distribution of reproduced copies of all TOP SECRET documents, of all classified documents covered by special access programs distributed outside the originating agency, and of all SECRET and CONFIDENTIAL documents that are marked with special dissemination and reproduction limitations.

THIS PAGE INTENTIONALLY LEFT BLANK

SECTION 8. ADP SECURITY (U)

8.1 General (U)

(U) This section presents the ADP considerations necessary to provide requisite computer and network security. The requirements are derived from DCID 1/16.

8.2 Hardware (U)

8.2.1 (U) Design, Development, Installation, Maintenance, and Modification. All hardware will be procured and distributed by the CHOSUN program office. All hardware will be tested for stand-alone operation and for network operation within the CHOSUN design, engineering, and integration facility prior to delivery and installation at a node. Initial installation at a site will be done by the CHOSUN contractor under the cognizance of the CHOSUN program management office and persons responsible for security at that site.

(U) Maintenance of the hardware will be coordinated with the CHOSUN NSO, NISSO, or HISSO affected. A record of all visits by maintenance personnel shall be made and retained for one (1) year. (See section 5, Personnel Security, and section 6, Physical Security, for specific clearance requirements for maintenance and service personnel.)

(U) Modification to the hardware must not be undertaken independently by the nodes. Any modifications that are deemed necessary must be reviewed and approved by the CHOSUN NCWG in accordance with the CHOSUN Configuration Management Plan. Major modifications will require recertification of the network by the NCWG and reaccreditation by the DAA. (See section 4.10, Schedule for Recertification and Reaccreditation.

8.2.2 (U) Configuration Management. The CHOSUN program office will provide all sites with a SOP manual that contains a detailed checklist of procedures to be employed by the nodes. This includes the setting of all hardware switches, the powering up and down of each individual device, the loading of the configured system with standard software and firmware, system operating procedures, and shutdown and restart procedures.

(U) The SOP will also include the optional procedures for purging and disconnecting components of the node system in order to interface with ADP systems or communications networks outside the CHOSUN network which may be operating at a lower classification level. (A "port-connected" alert will be placed on all conference User Control

Terminals (UCTs) for all word processing or graphic external interconnections.) In addition, procedures for reconnecting node components, after processing at a lower classification level, will be included. The SOP is primarily an operations manual, but its existence and strict adherence to the procedures it sets forth are essential to overall system security.

(U) Where node procedures vary from the SOP, each node is responsible for preparing and submitting for NCWG review the text for node-unique procedures. With the concurrence of the NCWG, node-unique procedures will be included as an addendum to the SOP. Any proposed changes to the standard hardware/software may impact operational procedures. Therefore, as previously stated, all proposed changes will be reviewed and evaluated by the configuration manager at the nodes and submitted to the NCWG for approval before incorporation into the SOP.

(U) A unique SOP will be developed for use at the hub. The topics covered will be the same, but hub specifics will differ.

8.2.3 (U) System Clearing Procedures. At the termination of a conference, all user data will be purged from the system. This will normally include all removable media. In special cases, and then only with the concurrence of the conference originator, removable media may be removed before the clearing process. After system clearing, removable media will be removed, marked appropriately if not marked, and stored in a secure container. Clearing of memory will be initiated by software at the hub.

8.3 Software (U)

(U) Software utilized in CHOSUN will be largely off-the-shelf software with a limited amount of software newly developed by the vendor. This section describes the procedures for developing, testing, and controlling the software.

8.3.1 (U) System and Application Software Design, Development, Installation, Maintenance, and Modification. All software utilized within the CHOSUN network will be provided by the CHOSUN program office. Sites may not modify or add to the software package provided.

(U) The system consisting of commercial and newly developed software must be tested and shown to satisfy the CHOSUN security requirements.

(U) All CHOSUN-developed software must be developed in a secure environment and maintained under strict configuration management. Those personnel responsible for the design and development of

software have the best knowledge of its possible weaknesses. Therefore, all personnel (contractor and Government) who are involved in the design and/or development of any software that is not commercially available, shall have as a minimum, a TOP SECRET clearance. Work shall be done in a classified environment and all listings shall be labeled SECRET.

a. (U) Security specifications for each new system release will be developed by the Program Management Office, coordinated with the NSO, and approved by the NCWG prior to development.

b. (U) In-process design reviews for new system releases will be conducted by the Program Management Office in coordination with the NSO and NCWG to ascertain that the proposed design meets the approved specifications. The results of the design review will be fully documented and maintained as official records of the Program Management Office.

c. (U) System tests of new system releases will be conducted by the Program Management Office to demonstrate the functionality and stability of the new system release and that the system meets the approved security specifications. Tests will be designed by the Program Management Office, coordinated with the NSO, and approved by the NCWG. For the purposes of this testing, it will be assumed that the security features of the software can be penetrated under serious and sustained efforts. The purpose of these tests will not be to prove the integrity of the software and its ability to withstand penetration efforts but rather to ascertain that the security features function correctly under normal constraints. The testing should answer questions such as:

(1) (U) Is residue on scratch mass storage cleared during allocation?

(2) (U) Do security caveats print correctly?

(3) (U) Are users and terminals properly identified?

(4) (U) Does the system properly detect and respond to security incidents?

(5) (U) Are all audit reports relating to security correct?

(6) (U) Do new security interfaces developed for this release function correctly?

(U) Testing shall be conducted on development copies of the system against unclassified test data bases. The volume and variety of test data and the extent of testing shall be sufficient to ensure that the system will function in a cohesive, identifiable, predictable, and reliable manner. Upon completion of the test, the test results will be fully documented and maintained as part of the official records of the Program Management Office. Prior to installation of new system releases, the NCWG will certify that the system meets the documented and approved specifications and that results of the test demonstrate that the security provisions are adequate.

(U) To preclude the inadvertent disclosure of classified information to maintenance personnel, any node undergoing maintenance will be offline from the network. In addition, any maintenance which requires accessing any system dumps will be performed by maintenance personnel with the requisite clearance to see any classified which may be contained therein (see section 5, Personnel Security). The NISSO/HISSO will be notified of all requirements for maintenance personnel, and a record of such visits will be made and retained for one year.

8.3.2 (U) Configuration Management. The software utilized at the nodes is limited to that supplied by the CHOSUN program office. All CHOSUN-developed software shall be classified SECRET. All new releases will be delivered and installed by contractor personnel supporting the CHOSUN Program Management Office. The NISSO shall be responsible for assuring that the software is stored in a secure container.

(U) The Program Management Office shall maintain an operational and a developmental set of system software. In addition, a prior release of the system shall be retained as backup. Backup copies of the operating system and utilities will also be available at all nodes and the hub. All proposed software modifications must be reviewed and approved in accordance with the CHOSUN Configuration Management Plan. The proposed change will be reviewed by the Configuration Review Board to determine if the proposed modification significantly affects security. All new software releases will be subjected to design reviews and testing as identified in section 8.3.1. Interrelease of individual changes (software patches) that significantly impact security shall be distributed only with the approval of the NSO after favorable evaluation of test results.

(U) A software modification shall be considered to significantly affect security if modules performing any of the following functions are being altered:

a. (U) Audit.

b. (U) Authentication.

c. (U) Labeling.

d. (U) User identification.

e. (U) Privacy keying.

8.4 Audit Trails (U)

(U) The NSO shall examine the audit trails for the network on a daily basis. The authority for any unexpected use of the network shall be investigated. The users identified by the system audit trail shall be compared to the facility lock audit trail.

(U) Audit trails shall be maintained at each node and at the hub, and shall be retained for one year. The audit trails should be kept in machine-readable form and may be consolidated if desired.

(U) The hub audit trail shall, at a minimum, record the following information:

a. (U) Date and time of conference.

b. (U) Identity of individual who scheduled the conference.

c. (U) Participants in conference (nodes).

d. (U) Duration of conference.

e. (U) Unclassified name of conference (assigned by scheduler).

f. (U) Classification of conference.

g. (U) Media used (e.g., voice, word processing).

h. (U) File and data tranfers, to include file name, sender, number of box pages or freeze-frame screens transmitted, and receiving users.

i. (U) Date authorized for release (i.e., printing, storing on a floppy disk).

(U) The node audit trail shall include, at a minimum, the following information:

a. (U) Date and time of conference.

b. (U) Participants (individuals) at the node.

c. (U) Name of conference.

d. (U) Identification and classification of media utilized as input or created as output.

e. (U) The classification, time sent, and destination of all data leaving the node.

f. (U) Date authorized for release (i.e., printing or storing on a floppy disk).

8.5 ADP Products and Storage Media (U)

8.5.1 (U) Marking, Storage, and Control/Accountability. All ADP products (e.g., printed listings, documents, hard copy printouts of CRT displays) and storage media (e.g., disk packs, magnetic tapes, diskettes) shall be marked, stored, and controlled in accordance with the requirements prescribed for the highest level of classification and sensitivity of any information contained in the product or stored on the media.

8.5.1.1 (U) Marking:

a. (U) ADP Products. All classified ADP products shall be marked as prescribed below. Detailed procedures are provided in section 7. In addition, to provide a means for controlling the products, all classified ADP products should also be marked with the originator and a unique identifier. To facilitate the proper safeguarding of products that cannot have their assigned classification/sensitivity immediately verified, the classification of the system environment in which the product was produced should also be clearly indicated on the front of the ADP product.

(1) (U) Printed Listings. Listings containing classified information shall be marked with the intended security classification on the top and bottom of each page. The classification markings may be applied by the ADP

equipment or by other means. The front cover should be marked with the safeguard statement as shown in figure 8-1. Each page should be appropriately numbered, and the user is responsible for checking the continuity of page numbering as soon as practicable after receipt. This review will reduce the possibility of accidental distribution of material classified at a higher level than the basic listing.

(2) (U) CRT Displays. The system shall display the appropriate classification level and caveats on the CRT screen when a file is initially opened. If a hard copy of the CRT display is made, the user is responsible for adding the required security classification at the top and bottom of each page.

b. (U) Storage Media. All storage media (e.g., magnetic tapes, disks, disk packs, diskettes) shall be externally marked with their overall security classification, special access restrictions, and a permanently assigned identification/control number.

(1) (U) Magnetic Tapes. In addition to the above-stated minimum requirements, each magnetic tape shall have a gummed label affixed containing, at least, the name of the owner of the tape, date of creation, tape classification, identification of the tape contents, and the tape identification/control number.

(2) (U) Removable Disk Packs. Removable disk packs shall be marked with the same information required for magnetic tapes. The identification control number shall be marked directly on the hub of the disk pack. CAUTION: Care must be taken not to attach any labels that would destroy the balance of the disk pack and cause a disk crash. Use of a magic marker is best for marking the pack itself. Gummed labels shall be affixed to the top of the disk pack cover to control information.

(3) (U) Other Media. All other media shall be conspicuously marked on their covers with the minimum information described above.

8.5.1.2 (U) Storage. All classified information (ADP products and storage media) must be stored in accordance with requirements for the highest classification and sensitivity of the information being

SAFEGUARD STATEMENT

* * * SAFEGUARD * * *

HANDLE AS TOP SECRET SI/ / / INFORMATION UNTIL SIGNED BY INDIVIDUAL WHO HAS DETERMINED THAT THE SECURITY CLASSIFICATION OF THIS DOCUMENT IS APPROPRIATELY MARKED AND THAT THE DOCUMENT CAN ASSUME THE HANDLING REQUIREMENTS FOR THAT CLASSIFICATION. REPORT ANY UNUSUAL OR UNREQUESTED OUTPUT DISCREPANCIES IMMEDIATELY TO: (INFORMATION SYSTEM SECURITY OFFICER, ROOM NUMBER, PHONE NUMBER). I HAVE REVIEWED THIS DOCUMENT AND BASED ON THE CONTENT FOUND IT SHOULD BE CLASSIFIED: _____

SIGNATURE _____ DATE _____

UNCLASSIFIED

Figure 8-1. (U) Safeguard Statement

stored. Facilities for both open and closed storage of classified information may be provided at each node. The NISSO will be responsible for determining what information may be maintained in an open storage facility. All other classified information, to include all storage media and all network/system software, will be maintained in a closed storage facility. Section 7.5, Storage and Safekeeping, states the security requirements for the storage and safekeeping of classified information.

8.5.1.3 (U) Control and Accountability. Control and accountability procedures must be established for all classified information. General procedures for control and accountability of ADP products and storage media are provided below. Detailed procedures are provided in section 7.6, Accountability and Control.

a. (U) ADP Products. The user shall receipt for all classified material received from the network. The user is responsible for initiating formal accountability controls for the products received. ADP products will be marked on their front cover with a safeguard statement (see figure 8-1). The user will be responsible for protecting ADP products marked with the safeguard statement as appropriate for the highest classification and all categories of data that were contained in the ADP system at the time the product was produced. After reviewing the output product, verifying its actual classification, and completing the safeguard statement, the customer may control the product at its actual classification.

b. (U) Storage media. Procedures for maintaining an inventory of all removable storage media shall be established. As a minimum, the inventory listing should contain the identification/control number, the highest security classification/special category caveats, and date of creation of the device. The inventory listing shall be verified at least annually. Devices classified SECRET and below should also be verified at least annually.

8.5.2 (U) Erase, Declassification, and Destruction Procedures.

8.5.2.1 (U) Erase Procedures. At the end of each conference, each memory location of the processor and the special devices shall be overwritten to preclude the unauthorized disclosure of classified data. The CHOSUN network software will provide the capability for automatically overwriting areas of memory and the disks which may be used to store data. Erased memory units and storage media must still be protected in accordance with the requirements for the highest classification and sensitivity of the information that

was stored, until the declassification procedures outlined in section 8.5.2.2 have been applied.

8.5.2.2 (U) Declassification Procedures. Each node shall have on site the necessary programs, equipment, and procedures for declassifying all ADP equipment that may be used for processing or storing classified material.

(U) When any of the memory units or storage media are removed from the controlled environment, the following declassification procedures apply:

a. (U) Magnetic Tapes. Appendix I lists the names and model numbers of magnetic tape erase equipment that are approved for declassifying magnetic tapes. Detailed specifications for erasing magnetic storage media are contained in appendix J, Specifications for Magnetic Tape Erase Equipment.

b. (U) Magnetic Disks and Disk Packs (Operative). When the capability exists as an integral part of the storage subsystem, an AC/DC erase will be applied to all data tracks before the tracks are overwritten a minimum of three times and the overwrite is verified. Appendix K lists approved disk/disk pack degaussers. Thereafter, all storage locations will be overwritten a minimum of three times: once with the binary digit "1," once with the binary digit "0," and once with a single numeric, alphabetic, or special character. Such alphanumeric or other UNCLASSIFIED data shall be left on the device. The current electrical used in overwriting must be equal to or greater than that used in recording the information, but of a strength that will not damage or impair the equipment.

c. (U) Magnetic Disks and Disk Packs (Inoperative). If the storage media has failed in such a manner that it cannot be overwritten, the media may be declassified by one of the following methods:

(1) (U) Expose the recording surface(s) to a permanent magnet having a field strength at the recording surface of at least 1,500 oersted. Care must be taken to ensure that the entire surface is wiped at least three times by a nonuniform motion of the magnet. Care must also be taken to assure that all tracks are covered by the center of the magnet. A thin sheet of clear plastic (1-5 mil sheet) should be used to prevent damage to the recording surface(s).

(2) (U) Disassemble the platters from the disk pack. Sand off the recording surfaces on both sides of the platter.

(3) (U) Disassemble the platters from the disk packs. Use a torch and burn off the recording surfaces on both sides of the platters.

(4) (U) Disassemble the platters from the disk pack. Sand off the recording surfaces on both sides of the platters and spray paint the recording surfaces.

d. (U) Internal Memory. Hardware/software techniques for the declassification of internal memory will be provided as part of the system. See section 8.2.3, System Clearing Procedures.

e. (U) Magnetic Storage Media Used To Store Analog, Video, or Similar Nondigital Information. Magnetic tape used to record analog, video, or similar types of nondigital information may be declassified by degaussing as in paragraph 8.5.2.2.a Rigid magnetic storage surfaces may be declassified as in paragraph 8.5.2.2.b above, except that the UNCLASSIFIED overwriting signal must be analog instead of binary, with the latter recording left intact on the device. In the case of a failure of the degausser or the overwriting methods, a permanent magnet may be used as in paragraph 8.5.2.2.c above for rigid recording surfaces.

8.5.2.3 (U) Destruction Procedures. Appendix L specifies approved devices for the physical destruction of all classifed paper waste. In addition, the following paragraphs define the procedures for the destruction of classified ADP products and storage media.

a. (U) ADP Products. Classified documents and material shall be destroyed by burning, or with the approval of the NISSO/ HISSO by melting, chemical decomposition, pulping, pulverizing, shredding, or mutilation sufficient to preclude recognition or reconstruction of the classified information. Records of destruction are required for compartmented, TOP SECRET, and SECRET information. The record shall be dated and signed at the time of destruction by two witnesses for compartmented and TOP SECRET information and one witness for SECRET. In the case of information placed in burn bags for central disposal, the destruction record need only be signed by the witnessing official or officials when the information is so placed. Records of destruction shall be maintained for a minimum of two years. In individual cases involving

SECRET information, the NISSO/HISSO may waive the requirement for destruction records if compliance would create an unacceptable degree of operating inefficiency.

(U) Classified waste, such as handwritten notes, carbon paper, printer ribbons, and working papers, shall also be destroyed when no longer needed by a method described above. Destruction records are not required.

b. (U) Storage media. Storage media that cannot be declassified in accordance with section 8.5.2.2 Declassification Procedures, may be destroyed by burning or, with the approval of the NSO, by melting, chemical decomposition, pulping, pulverizing, shredding, or mutilation.

8.5.2.4 (U) Disposition/Destruction Approval. With the specific approval in each case of the NISSO, storage media declassified in accordance with the procedures described in paragraph 8.5.2.2 may be handled as UNCLASSIFIED and released as necessary.

(U) A record of the declassification of storage media and the NISSO/HISSO approval shall be maintained for a period of two years after disposition of the devices or equipment.

(U) Guidance for the declassification of storage media not covered in section 8.5.2.2 may be obtained by submission of all pertinent details to the NSO for consideration on a case-by-case basis.

(U) In the absence of data eradication by approved equipment or procedures, or at the direction of the NSO, storage media shall be safeguarded in the manner prescribed for the highest classification, and for each special category, ever recorded thereon until it is destroyed.

(U) All labels and security classification markings shall be removed from the magnetic storage media after declassification but before release as UNCLASSIFIED.

8.6 Access Controls (U)

8.6.1 (U) General. Each individual user of the system, including personnel utilizing CHOSUN word processing equipment, will have a unique UNCLASSIFIED USERID assigned. The NSO is responsible for maintaining USERIDs, as well as generating and distributing the log-on passwords for each USERID for network access. In addition, the NISSO is responsible for generating and distributing USERIDs and log-on passwords for the word processor at the node. All passwords will be stored in an approved security container. A password-gene-

rating program may be utilized if approved by NSA.

(U) Official requests for individual(s) access will be submitted in accordance with the procedures identified in section 5. The NSO will act as central custodian of all system/network access authorization requests and will notify the appropriate NISSO/HISSO or PMO of approvals/disapprovals. The NISSO/HISSO will install a USERID and password on the node's word processor for each CHOSUN user for his node.

8.6.2 (U) Changes. Log-on passwords will be deleted or changed under any of the following conditions:

a. (U) When an individual's access is withdrawn for any reason (e.g., transfer, discharge, reassignment). In a normal situation, individual access is withdrawn before clearance is revoked.

b. (U) When a password or record of passwords has been compromised or is suspected of being compromised.

c. (U) At least semiannually.

8.7 Security Incidents (U)

(U) All security incidents will be investigated by the NISSO/HISSO to determine their cause and, where possible, corrective action will be taken. In addition, all incidents affecting one or more nodes will be reported to the NSO. The FBI will report all Soviet Bloc threats to the National Security Council and then to the individual agency NISSO. All incidents will be fully documented so that areas requiring special corrective action can be identified. If it is determined that a compromise of classified information may have occurred, a report of facts surrounding the incident shall be immediately forwarded by the NSO to the NCWG for evaluation. The preliminary investigation conducted by the NSO may be followed by a formal investigation by the NCWG if required. The NCWG will determine if system/network recertification is required. Individual investigation reports will be maintained for three years.

8.8 Contingency Operations Plans (U)

8.8.1 (U) General. The procedures established in previous sections for personnel, physical, information, communications, and ADP security have been formulated to protect against deliberate attempts to compromise the CHOSUN network, as well as those contingencies for which safeguards may be implemented to protect against permanent destruction, extended loss, or degradation of the node/hub network

capabilities.

(U) While high reliability of the node systems and the network is critical, the availability of alternative communications media, the close geographical proximity of the nodes, and the limited amount of space at the nodes and hub militate against complete redundancy of all equipment at all facilities.

8.8.2 (U) NISSO/HISSO Involvement. Due to the criticality of the planning required for continuity of operations, the NISSO/HISSO will be responsible for the formulation and periodic testing of the node contingency plans. All test results will be forwarded to the NSO for review and evaluation.

SECTION 9. COMMUNICATIONS SECURITY, PRIVACY, AND EMANATIONS SECURITY (U)

9.1 General (U)

(C) Due to the extreme sensitivity of the information handled by the CHOSUN network, positive measures to protect the electrical information from disclosure to unauthorized persons must be taken. These measures are grouped into three categories: Communications Security (COMSEC), privacy, and Emanations Security (EMSEC).

9.2 Communications Security (U)

9.2.1 (C) Encryption. To ensure adequate communications security, all signals leaving each node and the hub switch facility shall be encrypted using KG-81 cryptographic equipment. This equipment will be installed and operated in accordance with KAO-179A/TSEC, "Operating Instructions for the KG-81 in the CI-3 System, and TRI-TAC." The keying material to be used for the KG-81s shall be TS/SCI and must be protected by storage in a GSA container approved for TOP SECRET or in a Class A vault.

9.2.2 (U) COMSEC Custodian. Each node and the hub facility will appoint a COMSEC custodian and alternate custodian. These individuals shall be responsible for the acquisition, storage, operation, maintenance, and safeguarding of all cryptographic materials at their installation. Custodians should be appointed in accordance with existing internal regulations of the agency involved.

9.2.3 (C) RED Technical Control Facilities. Since all RED technical control facilities process highly classified signals in the clear, all such facilities must be designed, installed, and operated in accordance with NACSIM 5203. Positive means must be taken to prevent either the inadvertent or deliberate connection of RED signals to BLACK communications facilities. Under no condition is the connection of RED signals (even though protected by Data Encryption Standard equipment) authorized to any public, private, or Government communications network. All signal connections to the Washington Area Wideband System (WAWS) must be on a BLACK basis.

9.3 Privacy (U)

9.3.1 (C) Data Encryption Standard (DES). To ensure privacy and protection of the need-to-know requirement, DES equipment will be used to further process classified information. It should be noted that the use of DES does not provide communications security for signals and hence any signals leaving the RED enclosure must be protected by cryptographic equipment or Protected Distribution Systems

(PDSs) in accordance with NACSIM 5203 and NACSI 4009. The DES is not approved for the protection of data classified by the National Security Act of 1947, as amended, or the Atomic Energy Act of 1954, as amended. The DES shall be implemented according to FIPS Pubs. 46 and 81. Since data protected by DES is still considered as classified information, more stringent means of protection than those required by FED STDs 1026 and 1027 are required (i.e., NACSIM 5203, NASCI 4009, and NACSEM 7002). In addition, all DES equipment and keying material will be protected as TOP SECRET.

9.3.2 (U) DES Custodian. Each node and the hub facility will appoint a DES custodian and alternate custodian. These individuals will be responsible for the acquisition, storage, operation, maintenance, and safeguarding of all DES material. These individuals will function similarly to the COMSEC custodians although the regulations governing this application of the DES have yet to be developed.

9.4 Emanations Security (EMSEC) (U)

(U) The Director of Central Intelligence (DCI) has directed in DCID 1/19 that, "all electronic equipment which is used to process or transmit SCI shall meet national standards for TEMPEST." Therefore, all CHOSUN facilities must be TEMPEST accredited.

(C) Compliance with the National Communications Security Committee's (NCSC) National Policy on the Control of Compromising Emanations is built into the CHOSUN system. There are three methods that may be used for controlling compromising emanations: first, to provide the equipment with a Controlled Zone (CZ) sufficient to preclude a successful hostile intercept action; second, to implement minimum-essential countermeasures to contain compromising emanations within the CZ; and third, to design or modify any equipment used to limit the strength of compromising emanations to acceptable limits considering the available CZ. In CHOSUN, the CZ is the walls, floor, and ceiling of the parent rooms within which are installed the RF-shielded cabinet/racks.

(S) The implementation approach, as presented in the contractor's proposal, for controlling emanations includes:

a. (S) An RF-shielded conference room facility for housing the user consoles in a secure environment.

b. (S) Utilization of TEMPEST-approved racks/enclosure for housing support equipment, privacy devices, video compression equipment, and control processor equipment.

c. (U) Utilization of an approved protected distribution system to distribute the CHOSUN signals within a node facility.

(C) In addition, it is mandatory that all digital signals conform to NACSI 5002, "Suppression of Compromising Emanations Through Low Level Operation," or be installed using the requirements and methods of Chapter 6, NACSIM 5203.

9.4.1 (U) Facility Design. All CHOSUN facilities shall be designed and built in strict accordance with NACSIM 5203 and NACSI 4009. Protective measures that must be taken are delineated in NACSI 5004, "TEMPEST Countermeasures for Facilities Within the United States." More stringent measures, as determined by local authorities, may be imposed.

9.4.2 (C) Future Equipment Design, Testing, and Certification. All future equipment which will be used for processing RED CHOSUN information and not planned for installation within an RF-shielded room or RF-shielded equipment cabinet/racks, shall meet the requirements specified in a. or b. below:

a. (U) Meet the baseline emanation limits established by NACSIM 5100A, or

b. (U) Be modified after TEMPEST tests to provide an equivalent level of protection as that provided by NACSIM 5100A.

(U) For specific equipment planned for installation in a non-RF-shielded environment, the provisions of NACSEM 5201, "TEMPEST Guidelines for Equipment/System Design," apply to all new equipment specifically designed and constructed for use in CHOSUN.

(U) A Preferred Products List (PPL) is prepared by the TEMPEST Qualification Special Committee (TQSC) of the Subcommittee on Compromising Emanations (SCOCE), NCSC. Equipment appearing in the PPL indicate compliance with the requirements of NACSEM 5100 or NACSIM 5100A and wherever possible should be selected for use in CHOSUN when installed in a non-RF-shielded environment.

9.4.3 (U) TEMPEST Testing. All CHOSUN equipment and facilities processing classified information shall be tested for compliance with NACSIM 5100A. Newly installed equipment will require that testing be accomplished before node recertification can be given.

(U) In addition to review and approval of the implementation contractor's TEMPEST Control Plan, the Government and a representative of the NCWG will witness all TEMPEST-testing activities performed by the contractor at the nodes and hub.

9.4.4 (C) Protected Distribution System. NACSI 4009 requires that all signal distribution lines that carry classified data shall be accomplished via a PDS and installed in accordance with NACSIM 5203.

9.4.5 (C) Acoustics Emanation Protection. Protection against acoustical emanations shall be accomplished in accordance with NACSIM 5103 for all CHOSUN nodes/facilities that process classified information.

9.4.6 (U) Other Considerations

9.4.6.1 (U) Electromagnetic Interference (EMI). All equipment, both RED and BLACK, installed or used within the CHOSUN network, shall meet the requirements of Military Standard (MIL-STD)-461.

9.4.6.2 (U) Electromagnetic Compatibility (EMC). All equipment, both RED and BLACK, installed or used within the CHOSUN network shall meet the requirements of MIL-STD-462.

9.4.6.3 (U) Personally Owned Electronic Equipment. In order to maintain the TEMPEST integrity of CHOSUN facilities, the introduction of personally owned electronic equipment such as radios, televisions, tape recorders, or computers into any CHOSUN facility is strictly prohibited.

SECTION 10. SECURITY TESTING (U)

10.1 General (U)

10.1.1 (U) Purpose. While Security Test and Evaluation will be a part of the certification process, a continuous security testing program is necessary to maintain a secure environment and a high security posture. Accordingly, it is essential that all aspects of CHOSUN security be tested on a thorough and frequent basis; these tests shall occur on both a scheduled basis and on unannounced occasions in order to provide continuing evidence of the effectiveness of the in-place security features.

10.1.2 (U) Responsibility. It is the responsibility of the Network Security Officer to ensure that appropriate security testing is carried out for CHOSUN; this testing shall be comprised of two major elements: preplanned testing and unannounced spot-check testing. Results of all test activities will be reviewed and evaluated by the NSO, and any resultant recommendations for additional, enhanced security protection will be forwarded to the NCWG.

10.2 Preplanned System/Network Tests (U)

(U) The NSO is responsible for development of a comprehensive security test program for CHOSUN to be approved by the NCWG. The NSO will work with the NISSOs and HISSO in order to coordinate individual, scheduled test periods and site visits relative to various aspects of the test plan. The NISSOs/HISSO are responsible for documenting the results of the testing activities and forwarding results to the NSO.

10.2.1 (U) Test Scope. The NSO is responsible for development of policy and procedures for security testing. Within the node/hub element, testing activities/audit activities will be conducted to include, at a minimum:

a. (U) Verify on-site availability of all current-issue CHOSUN security documentation and procedural knowlege by the NISSOs/HISSO.

b. (U) Perform periodic on-site inspections to ensure physical integrity of all CHOSUN facilities, such as equipment/equipment bays, and the protected distribution system.

c. (U) Perform periodic on-site TEMPEST tests to ensure absence of compromising emanations. Newly installed equipment, or the modification of existing equipment,

will require that on-site TEMPEST testing be reaccomplished prior to the activation of the site and the issuance of a new site certification.

d. (U) Review/verify completeness of all information accountability records, as well as procedures/facilities for information storage and/or destruction.

e. (U) Review/verify completeness of system access logs (e.g., operator, maintenance personnel) for nonuser personnel.

f. (U) Conduct periodic checks on all "alarmed" elements (e.g., intrusion detection system, external "ports" from consoles).

g. (U) Review/verify node/hub roster for all nonuser personnel authorized for CHOSUN access.

10.2.2 (U) Test Schedule and Frequency. Periods in which tests are to be performed within the node/hub elements will be coordinated between the NSO and the cognizant NISSO/HISSO. In no case should security testing activities take priority over operational use of the CHOSUN network; local or network security tests in progress when operational use is required shall be immediately suspended.

(U) Since security testing is a continuous process, there is no one assigned frequency of repetition for the testing activities as discussed in section 10.2.1. It is expected that the range will vary from a minimum of once daily for alarm systems to once every three months for review/audit of accountability logs. Minimum-prescribed frequencies of performance will be set in the Network Security Test Plan.

10.2.3 (U) Resources. Personnel augmentation, if any, necessary to perform the test activities within a node/hub element is the responsibility of the NSO, through close coordination/cooperation among the NSO and NISSOs/HISSO. It may be desirable to form a network test team to perform all testing activities. If the team concept is accepted, test team members should be selected in order that all of the following areas of expertise are represented:

a. (U) Procedural security doctrine.

b. (U) Personnel security.

c. (U) Physical security.

d. (U) Communications/emanations security.

e. (U) Computer security.

f. (U) Threat/exploitation currency.

10.3 Unannounced Random System Tests (U)

(U) In addition to the scheduled preplanned system tests discussed in section 10.2, there will be unannounced spot checks of any/all security features of the CHOSUN network. These tests will be authorized by the NCWG, though the NSO is responsible for scheduling the test times.

10.3.1 (U) Test Scope. The scope of potential test activities for the unannounced security tests and spot checks is identical to that of the preplanned tests (section 10.2).

10.3.2 (U) Test Schedule. Tests will be conducted as directed by the NSO. As in the case of preplanned testing, any unannounced security test will be suspended immediately if operational use of the local CHOSUN element is needed.

10.3.3 (U) Resources. Resources to conduct unannounced tests are the sole responsibility of the NSO. As discussed for preplanned tests, it may be desirable to develop a network security team with qualified membership in order to most effectively support the unannounced checks.

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX A

DEFINITION OF TERMS (U)

THIS PAGE INTENTIONALLY LEFT BLANK

Access (Data). The ability to receive products created or transmitted by the system; implies no form of direct communication with the system.

Access (Physical). The ability or means to enter a controlled area.

Access (System). The ability to communicate with (input to or receive output from) the system; implies physical access to the system.

Access Code. A software feature designed to detect and prevent unauthorized use (and permit authorized use) of the system.

Access Control. The process of limiting physical access to the system (and system access to the resources of the system) to authorized personnel.

Accreditation (Approval). The authorization and approval granted to a system or network to process sensitive classified data in an operational environment. Accreditation of the system will be made on the basis of certification by the Network Certification Working Group that designated technical personnel have examined and verified that the design (all network hardware and software) and implementation of the system meet prescribed technical and procedural requirements for achieving adequate system/data security.

Accreditation Authority. See Designated Approving Authority.

Audit. To conduct the independent review and examination of system records/activities in order to test for adequacy of system controls, to ensure compliance with established policy and operational procedures, and to recommend any indicated changes in controls, policy, or procedures.

Audit Trail. A software feature providing a chronological record of system activities/functions that when reviewed/monitored gives an accurate account of usage or user activity within the system.

Authentication. The software feature which verifies user eligibility to access the system.

Authorization. The granting to a user the right of access 1) to the a controlled area or 2) to the system within the controlled area.

Backup Procedures. The provisions made for recovery of data and for restart or replacement of equipment after degradation or loss of the system. Also see Contingency Plans.

Certification. The technical process, made as part of and in support of the accreditation process, whereby a procedure, hardware/software component, system, or network is established as meeting prespecified security requirements.

Classification. The determination that official information requires, in the interests of national security, a specific degree of protection against unauthorized disclosure, coupled with a designation signifying that such a determination has been made.

Closed Storage. The storage of sensitive compartmented information and material in properly secured General Services Administration (GSA) approved security containers within an accredited facility when the facility is not occupied by authorized personnel.

Communications Security (COMSEC). The protection (hardware and software) that ensures the authenticity of telecommunications and that results from the application of measures taken to deny unauthorized persons any information which might be derived from the acquisition of telecommunications.

Compartmented Intelligence. See Sensitive Compartmented Information.

Compromise. The unauthorized disclosure or loss of sensitive/classified information.

Compromising Emanations. Unintentional data-related or intelligence-bearing signals which, if intercepted and analyzed, disclose classified information being transmitted, received, handled, or otherwise processed by any information-processing equipment.

Computer Facility. One or more computer systems with their peripheral devices, technical controls, and communications equipment in a single controlled area.

Configuration Control. See Configuration Management.

Configuration Management. The engineering management procedure that includes the following elements:

a. Configuration Identification. Selection of the documents which identify and define the configuration baseline characteristics of an item.

b. Configuration Control. Controlling changes to the configuration and its identification documents.

c. Configuration Status Accounting. Recording and reporting the implementation of changes to the configuration and its identification documents.

d. Technical Review. The method by which the contractor and Government determine that the development of a configuration item has reached contract milestone requirements.

e. Configuration Audit. Checking an item for compliance with the configuration identification.

Contingency Plan. A plan which details alternative operational procedures for performing functions which can no longer be performed due to degradation or loss of the system.

Controlled Access. See Access Control.

Control Zone. The physical space that surrounds equipment that is used to process sensitive defense/political information and that is under sufficient physical and technical control to preclude unauthorized entry or compromise.

Countermeasure. A security feature or control (e.g., hardware/software, personnel, physical, communications, or administrative) designated to reduce or eliminate security threats to the system.

Cryptographic System. A system which uses NSA cryptographic equipment that is directly connected to a signal line, making continuous processes of encryption and transmission or reception and decryption.

Data Security. The protection of data from accidental, unauthorized, intentional, or malicious modification, destruction, or disclosure.

Declassification. The determination that classified information no longer requires, in the interest of national security, any degree of protection against unauthorized disclosures, together with a removal or cancellation of the classification designation.

Derivative Classification. A determination that information is in substance the same as information currently classified, and the application of the classification markings.

Designated Approving Authority (DAA). The person designated to approve/accredit the CHOSUN network for the processing, use, storage, production, and transmission of sensitive/classified information.

Downgrade. A determination that classified information requires, in the interest of national security, a lower degree of protection against unauthorized disclosure than currently provided, together with a changing of the classification designation to reflect such a lower degree of protection.

Electromagnetic Emanations. Signals transmitted as radiation through the air and through conductors.

Emanations Security (EMSEC). The protection resulting from all measures designed to deny unauthorized persons information of value which might be derived from intercept and analysis of compromising emanations.

Encryption (End-to-End). Encryption of information at the origin within a communications network and decryption occurring at the final destination point.

Encryption (Link). The application of on-line crypto operations to a link of a communications system so that all information passing over the line is encrypted.

Escort. A designated person who has the appropriate clearance (TS/SCI) and access authorization for material processed, stored, and transmitted by the system and is sufficiently knowledgeable to understand the security implications of and to control the activities of an individual who does not have the appropriate clearance for unescorted access.

Hardware Security. Computer equipment features or devices used in the system to preclude unauthorized access to data or system resources.

Hub. The central switching facility for CHOSUN which links all nodes in the network.

Hub Information System Security Officer (HISSO). The individual designated to provide general supervision, administration, and overall coordination of security matters for the Hub to include System Control, Network Control, and Central Technical Control elements.

Information Security. The result of any system of administrative policies and procedures for identifying, controlling, and protecting from unauthorized disclosure, information whose protection is authorized by executive order or statute.

Keying Materials. In cryptography, those devices which control the operations of encryption and decryption.

Mode of Operation. The security environment and method of operating the system. Also see System High.

Need-to-Know. The necessity for access to, knowledge of, or possession of classified or other sensitive defense information in order to carry out official military or other governmental duties. Responsibility for determining whether a person's duties require that he possess or have access to certain information, and whether he is authorized to receive it, rests upon the individual having current possession, knowledge, or control of the information involved and not upon the prospective recipient.

Network. The interconnection of the CHOSUN systems together with the necessary communications support.

Network Certification Working Group (NCWG). The organization designated to perform certification of the CHOSUN network.

Network Security Officer (NSO). The person designated to provide general supervision, administration, and overall coordination of CHOSUN system security matters, including operations, test, and evaluation.

Node. A computer facility at the user's location.

Node Information System Security Officer (NISSO). The individual designated to provide general supervision, administration, and overall coordination of node security matters.

Open Storage. The storage of classified information on shelves, in metal containers, locked or unlocked, but not in GSA-approved secure containers, within an accredited facility while the facility is not occupied by authorized personnel.

Operational Network. A network used to provide intercomponent transfer of operational traffic (e.g., data, graphics, video) between nodes.

Operator. A person technically qualified to perform certain functions on the system. Also see Technical Control Operator.

Original Classification. An initial determination that information requires, in the interest of national security, protection against unauthorized disclosure, together with a classification designation signifying the level of protection required.

Parent Room. The space located inside a building structure, within which is assembled either an RF-shielded enclosure or one or more RF-shielded cabinet/racks.

Personnel Security. The procedures established to ensure that all personnel accessing the system have the appropriate clearance and authorization.

Physical Security. That part of security concerned with the physical measures designed to safeguard personnel, to prevent unauthorized access to equipment, facilities, material and documents, and to safeguard them against espionage, sabotage, damage, and theft.

Procedural Security. The management constraints; operational, administrative and accountability procedures; and supplemental controls established to provide an acceptable level of protection for sensitive defense information and data.

Protected Distribution System (PDS). A telecommunications system which has been approved by a legally designated authority and to which electromagnetic and physical safeguards have been applied to permit safe electrical transmission of unencrypted sensitive information.

RED/BLACK Concept. The concept that electrical and electronic circuits, components, equipment, systems, and so forth, which handle classified plain language information in electric signal form (RED) be separated from those which handle encrypted or unclassified information (BLACK). Under this concept, RED and BLACK terminology is used to clarify specific criteria relating to, and to differentiate between, such circuits, components, equipment, systems, etc., and the areas in which they are contained.

Regrade. A determination that classified information requires a different degree of protection against unauthorized disclosure than currently provided, together with a change of classification designation that reflects such different degree of protection.

SECRET. National security information or material requiring a substantial degree of protection, the unauthorized disclosure of which could reasonably be expected to cause serious damage to the National security.

Security Incident. Any incident involving classified information in which there is a deviation from the requirements of governing security regulations. (Compromise, inadvertent disclosure, need-to-

know violations, and administrative deviation are examples of a security incident.)

Security Test and Evaluation (ST&E). An examination and analysis of the security features of the system as they have been applied in an operational environment to develop factual evidence upon which an accreditation can be based.

Sensitive Compartmented Information (SCI). That intelligence information having special controls indicating restrictive handling for which systems of compartmentation or handling are formally established.

Sensitive Compartmented Information Facility (SCIF). An area, room, group of rooms, or installation which has been accredited by appropriate authority for storage, discussion, and/or processing of sensitive compartmented information.

Software Security. Those general purpose executive, utility, or software development tools, applications programs, and routines which protect data or information handled by the system and its resources.

System. The combination of all CHOSUN hardware, software, and firmware at a node or the hub.

System High. For CHOSUN the utilization of the network to process, store, or transmit Secure Compartmented Information (SCI) when the total system, to include the central facility (Hub), the node terminals, and all their connected peripheral devices, are secured in accordance with the requirements for the highest classification level of all types of SCI processed, stored, or transmitted therein.

TEMPEST. Short name referring to investigations and studies of compromising emanations. Sometimes used synonomously for the term "compromising emanations" (e.g., TEMPEST testing).

Terminal Area. The physical space within the control zone of each node housing the video/data consoles and peripheral devices of the system.

TOP SECRET (TS). National security information requiring the highest degree of protection, the unauthorized disclosure of which could reasonably be expected to cause exceptionally grave damage to the national security.

Unescorted. A person who has the appropriate clearance (TS/SCI) and access authorization for material processed, stored, and transmitted

by the system to preclude the necessity of an escort when accessing the system.

User(s). The primary person(s)/organization(s) who will utilize the system for the purpose of exchanging sensitive defense information with other users.

USERID. A unique group of alphanumeric characters that identifies a particular individual for the purpose of utilizing the system.

Violation. See Security Incident.

Vulnerability. The susceptibility of a particular system to a specific attack, and the opportunity available to a threat agent to mount that attack. A vulnerability is always demonstrable but may exist independently of a known threat. In general, a description of a vulnerability takes account of those factors under friendly control.

APPENDIX B

BIBLIOGRAPHY

Classified by: DCA 184W00224
Declassify on: OADR

THIS PAGE INTENTIONALLY LEFT BLANK

(U) This appendix provides the complete citation for all references contained within the CHOSUN Network Security Manual. The references are listed by the issuing department/agency for each document.

(U) The White House, National Policy on Telecommunications and Automated Information System Security, National Security Decision Directive 145, 17 September 1984, UNCLASSIFIED.

(U) The President, National Security Information, Executive Order 12356 of April 2, 1982, Federal Register, Vol. 47, No. 66, UNCLASSIFIED.

(S) National Security Council, Crisis Information and Management System (CIMS): Project Medusa (S), White House National Security Decision Directive 95, 18 May 1983, SECRET.

(U) Director of Central Intelligence, Minimum Personnel Security Standards and Procedures Governing Eligibility for Access to Sensitive Compartmented Information, DCID 1/14, 13 May 1976, UNCLASSIFIED.

(U) Director of Central Intelligence, Security of Foreign Intelligence in Automated Data Processing Systems and Networks (U), DCID 1/16, 6 June 1978, CONFIDENTIAL.

(U) Director of Central Intelligence, Computer Security Regulation (U), Attachment to DCID 1/16, 4 December 1984, CONFIDENTIAL.

(U) Director of Central Intelligence, Security Policy for Sensitive Compartmented Information (U), DCID 1/19, 28 June 1982, CONFIDENTIAL.

(U) Director of Central Intelligence, Security Policy Concerning Travel and Assignment of Personnel with Access to Sensitive Compartmented Information (U), DCID 1/20, 6 June 1978, CONFIDENTIAL.

(U) Director of Central Intelligence, U.S. Intelligence Community Physical Security Standards for Sensitive Compartmented Information Facilities (U), NFIB/NFIC-9.1/47, 23 April 1981, FOUO.

(U) Defense Intelligence Agency, Physical Security Standards for Sensitive Compartmented Information Facilities (U), DIAM 50-3, 20 August 1976, FOUO.

(U) Defense Intelligence Agency, Security of Compartmented Computer Operations (U), DIAM 50-4, 24 June 1980, CONFIDENTIAL.

(U) National Security Agency, Operating Instructions for the KG-81 in the CI-3 Systems, and TRI-TAC (U), KAO-179A/TSEC, 1 December 1974, CONFIDENTIAL.

(U) National Security Agency, Specification for RF-Shielded Enclosures for Communications Equipment: General Specifications (U), NSA Specification 65-6, Appendix B of NACSEM 5204, January 1979, CONFIDENTIAL.

(U) National Security Agency/Central Security Service, TEMPEST Security Program (U), NSA/CSS Regulation 90-5, 20 August 1980, CONFIDENTIAL.

(U) National Security Agency, Communications Security Equipment System Document, TSEC/KG-81 Family (U), CSEEB-35, CONFIDENTIAL.

(U) National Security Agency, Compromising Emanations Laboratory Test Standard, Electromagnetic (U), NACSEM 5100, March 1974, CONFIDENTIAL.

(U) National Security Agency, Shielded Enclosures (U), NACSEM 5204, January 1979, CONFIDENTIAL.

(U) National Security Agency, TEMPEST Guidelines for Equipment/System Design (U), NACSIM 5201, September 1978, CONFIDENTIAL.

(U) National Security Agency, COMSEC Guidance for ADP Systems (U), NACSIM 7002, CONFIDENTIAL.

(U) National Security Agency, Compromising Emanations Laboratory Test Requirements, Electromagnetics (U), NACSIM 5100A, 1 July 1981, CONFIDENTIAL.

(U) National Security Agency, Compromising Emanations Laboratory Test Standard, Acoustics (U), NACSIM 5103, CONFIDENTIAL.

(U) National Security Agency, Guidelines for Facility Design and RED/BLACK Installation (U), NACSIM 5203, 30 June 1982, CONFIDENTIAL.

(U) National Security Agency, Protected Distribution Systems (U), NACSIM 4009, 30 December 1981, CONFIDENTIAL.

(U) National Security Agency, TEMPEST Countermeasures for Facilities Within the United States (U), NACSIM 5004, CONFIDENTIAL.

(U) National Communications Security Committee, NCSC Policy Directive 14-2.

(U) Office of Management and Budget, Security of Federal Automated Information Systems, OMB Circular A-71, Transmittal Memorandum No. 1, 27 July 1978, UNCLASSIFIED.

(U) National Security Act of 1947, 61 Stat. 495, 26 July 1947.

(U) Atomic Energy Act of 1954, 68 Stat. 919, 30 August 1954.

(U) National Technical Information Agency, Telecommunications: Interoperability and Security Requirements for Use of the Data Encryption Standard in Physical Layer of Data Communications, FED-STD-1026, UNCLASSIFIED.

(U) National Technical Information Agency, General Security Requirements for Equipment Using the Data Encryption Standard, FED-STD-1027, 14 April 1982, UNCLASSIFIED.

(U) Department of Defense, Information Security Program Regulation, DoD 5200.1-R, August 1982, UNCLASSIFIED.

(U) Department of Defense, Security Requirements for Automatic Data Processing (ADP) Systems, DoD 5200.28, 18 December 1972, UNCLASSIFIED.

(U) Department of Defense, ADP Security Manual, DoD 5200.28-M, January 1973, UNCLASSIFIED.

(U) Department of Defense, Sensitive Compartmented Information TEMPEST Policy and Guidance (U), TCO/BCO DoD letter dated 15 May 1979, CONFIDENTIAL.

(U) Department of Defense, Military Standardization Handbook RED/BLACK Engineering - Installation Guidelines (U), MIL-HDBK-232, 14 November 1972, CONFIDENTIAL, (Superseded by NACSIM 5203).

(U) Department of Defense, Electromagnetic Emission and Susceptibility Requirements for the Control of Electromagnetic Interference, MIL-STD-461B, 1 April 1980, UNCLASSIFIED.

(U) Department of Defense, Electromagnetic Interference Characteristics, Measurement of, MIL-STD-462, 9 February 1971 (Int. Notice 4 dated 1 April 1980), UNCLASSIFIED.

(U) Department of Defense, Method of Insertion-Loss Measurement (U), MIL-STD-220A, UNCLASSIFIED.

(U) Department of Defense, Method of Attenuation Measurement for Enclosures, Electromagnetic Shielding, for Electronic Test Purposes (U), MIL-STD-285, UNCLASSIFIED.

(U) Department of Defense, General Specification for Filter, Radio Interference (U), MIL-F-15733, UNCLASSIFIED.

(U) National Fire Protection Association, American National Standard: National Electric Code, UNCLASSIFIED.

(U) National Bureau of Standards, Data Encryption Standard, FIPS PUB 46, 15 January 1977, UNCLASSIFIED.

(U) National Bureau of Standards, DES Modes of Operation, FIPS PUB 81, 2 December 1980, UNCLASSIFIED.

(U) Department of the Army, Automated Systems Security, AR 380-380, 15 April 1979, UNCLASSIFIED.

(U) Department of the Army, Control of Compromising Emanations (U), AR 530-4, CONFIDENTIAL.

(U) Department of the Army, Army Automation Management, AR 18-1, 15 August 1980, UNCLASSIFIED.

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX C

CHOSUN SECURITY CLASSIFICATION GUIDE (U)

TO BE DETERMINED

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX D

REQUEST FOR WAIVER (U)

THIS PAGE INTENTIONALLY LEFT BLANK

(U) This appendix provides a generalized form/format for a CHOSUN user node/facility to request a specific waiver from the network security policies and procedures stated herein. Waivers will be granted on a very limited basis in those instances where site-unique facility/operational limitations warrant, and are granted for a limited time only.

(U) The waiver form, to be completed and endorsed by the NCWG as part of the site certification process, is unclassified prior to being completed. Classification of the completed form will be determined based upon the actual content.

REQUEST FOR WAIVER

Date: _____

1. Name of site: _____

2. Site location: Rooms: _____

Building: _____

Address: _____

_____

3. Identification of requirement for which waiver is requested:

(Cite paragraph in Security Manual) _____

_____

_____

4. Specific reason for waiver request:

Remarks _____

_____

_____

5. Alternate compliance proposed:

_____

_____

_____

6. (Expected) Duration of waiver: _____ to _____

7. Steps being taken to eventually meet requirement:

_____

_____

_____

8. Other requirements implied:
(Cost, time, manpower, operational impact etc.)

_____

_____

_____

_____
NCWG Representative

_____
Security Officer

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX E

SECURITY TEST AND EVALUATION REPORT FORMAT (U)

THIS PAGE INTENTIONALLY LEFT BLANK

(U) This appendix presents a format for reporting results of the Security Test and Evaluation performed as part of the certification process for CHOSUN operation.

1. COVER SHEET

   - Organization/Agency, location
   - ST&E time span
   - Date of report
   - Classification of report/declassification schedule
   - Identification/signature of individual(s) responsible for ST&E as documented herein

2. INTRODUCTION AND EXECUTIVE SUMMARY

   - Project CHOSUN overview
     - Organization/Agency Role/Mission
   - Objective of the report
   - Report organization
   - Major evaluation findings and recommendation(s)

3. BACKGROUND

   - Established security standards, criteria or policies
   - Specific assumptions and definitions relative to ST&E
   - Specific scope of this ST&E

     (i.e., exact boundary conditions assumed for this site during ST&E)

   - ST&E Summary
     - Participants tests analysis
     - Tests
     - Analysis

4. MAJOR FINDINGS

- Assets
- Threats
- Exposures

} In place

- Control mechanisms
- Vulnerabilities
  - Residual - no action recommended
  - Requiring correction

5. RECOMMENDED CORRECTIVE ACTION(S)

- Identify action to correct cited vulnerability
  - Costs, priority, impact
  - Responsible element
  - Subsequent evaluation

Annex A - Detailed Configuration/Description of Site Security

Annex B - Test Plan

Annex C - Test Result(s)

Annex D - Site Checklist(s)

Annex E - Site Risk Analysis

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX F

SITE SECURITY CHECKLISTS (U)

THIS PAGE INTENTIONALLY LEFT BLANK

(U) This appendix provides generalized formats/suggested versions of individual site security checklists to be completed as an essential part of the site certification process. Unless otherwise indicated, the checklists are extracted from DIAM 50-3. Individal checklists are provided for:

A. (U) General Information

B. (U) Procedural/Administration Security

C. (U) Physical/Facility Security

D. (U) TEMPEST

E. (U) ADP Security

(U) These checklists are unclassified prior to data being entered. Classification of the completed checklists will be determined individually based upon their content.

(U) Reponsibility to complete the individual checklists lies with the Node/Hub Security Officer although the NCWG may elect to inspect/review any element within the scope of assets/procedures covered by these checklists.

THIS PAGE INTENTIONALLY LEFT BLANK

A. GENERAL INFORMATION

1. Name of Site: _____

2. Site Location: Rooms: _____

Building: _____

Address: _____

3. Node/Hub Security Officer: _____ TEL/AUTOVON: _____

Alt. Security Officer: _____ TEL/AUTOVON: _____

4. Reason for Site Certification: Original: _____

Renewal: _____

5. Duty Hours: 1) Continuous: _____

2) _____ to _____, _____ days of week

3) Other _____

6. For Original Certification:

1) Construction completed (Date) anticipated complete (Date)

2) Tech. Security Survey completed (Date)

3) TEMPEST Security Checklist completed (Date)

7. For Renewal of Certification:

1) Certification/Accreditation granted by (document/authority) on (Date)

2) Last Inspected by _____ on (Date)

Deficiencies _____

Corrected _____

_____

3) TEMPEST Certification/Accreditation granted by _____
on _____ (Date)

4) ADP Certification/Accreditation granted by _____
on _____ (Date)

5. Date Site Certification Requested: _____

Remarks: _____

_____

_____

_____
Node/Hub Security Officer

B. PROCEDURAL/ADMINISTRATION SECURITY

ADMINISTRATION

1. Node/Hub Security Officer: _____ AUTOVON/TEL: _____
   Alternative Security Officer: _____ AUTOVON/TEL: _____

2. Current/Most Recent Version of CHOSUN Security Documentation Available

   CHOSUN Network Security Manual _____
   Node/Hub Security Manual _____
   Node/Network Operating Procedures _____
   Node/Network Contingency Operations Plans _____
   Node Security Test Plan _____

3. CHOSUN Security Orientation:

   Date of Most Recent Course Completion: NSO _____
   Alt NSO _____

4. Program to Inform Local Security of CHOSUN

   Site Commander/Senior Executive Ops. Officer _____
   Briefed on _____
   By _____

Remarks:

_____
_____
_____

PROCEDURAL

1. The following standardized current issue briefings are maintained by NSO:

   CHOSUN Security Indoctrination (Type 1 - Users, Type 2 - Other)
   CHOSUN Security Debrief
   CHOSUN Security Overview

2. Node/Hub Security Manual Last Update _____

C. PHYSICAL/FACILITY SECURITY

7. *Description of surrounding area outside of building:*

a. Fence _____

b. Fence lighting _____

c. Fence guards _____

d. Relationship of building to surrounding area _____

8. *Building:*

a. Construction _____

b. Building access control. Continuous? _____ During security hours only?

c. Guards (Military) (Civilian) _____

(1) Clearances _____

(2) Frequency of checks _____

(3) Communications _____

(4) Emergency procedures _____

(5) Reserves _____

9. *Remarks:* _____

Facility Security

10. *Access control:*

a. Guards (Military) (Civilian) _____

b. Assigned personnel _____

(1) Clearances _____

(2) Communications _____

(3) Emergency procedures _____

(4) Reserves _____

11. *Windows:* _____

_____

12. *Ventilating ducts:* _____

_____

13. *Construction:*

a. Walls _____

_____

_____

b. Ceiling _____

_____

_____

c. Floor _____

_____

_____

14. *Soundproofing:* (all of the preceding) _____

_____

15. *False ceiling:*

a. Type _____

b. Distance between false and true ceilings _____

16. *Remarks:* _____

_____

_____

_____

Doors

17. *Number of entrances:* _____

18. *Types of doors used:*

a. Vault door (manufacturer, model number)_____

_____

b. Wood (thickness/hollow/solid) _____

_____

c. Wood w/metal (thickness of both door and metal covering; hollow, solid, metal on both sides)_____

_____

_____

d. Metal (thickness/hollow/honeycombed) _____

_____

e. Other _____

19. *Number and types of doors used for emergency exits:* _____

a. Vault door (manufacturer, model number)_____

_____

b. Wood (thickness/hollow/solid) _____

_____

c. Wood w/metal (thickness of both door and metal covering; hollow, solid, metal on both sides)_____

_____

_____

d. Metal (thickness/hollow/honeycombed) _____

_____

e. Other _____

20. *Type of lock:* (entrances)

a. Combination (manufacturer, model, and group number) _____

_____

b. Is the entrance door (if not a vault door) and/or the access control door equipped with a pneumatic door closer? Yes _____ No _____ (if no, why not)_____

_____

21. *Locks on inspection ports/windows:* (if any) _____

_____

_____

22. *Have hinges been properly secured on doors opening outward?* Yes _____ No _____

How? _____

_____

23. *Soundproofing:* (all doors) _____

_____

24. *Type of locking device used on emergency exits:*

a. Lock, describe _____

b. Metal strap or bar _____

c. Security deadbolt(s) _____

d. Panic hardware _____

e. Other, describe _____

_____

_____

25. *Type of access control device used during duty hours:*

a. Cypher lock _____

b. Key lock _____

c. Electrical release _____

d. Guard _____

e. Other _____

_____

_____

_____

26. *Is combination lock of vault door opening into non-secure area protected against tampering?*

No _____ Why? _____ Yes _____ How? _____

27. *Combination changed by:* _____

on _____

28. *Combination on file at:* _____

29. ***Double check system:*** _____

_____

30. ***Remarks:*** _____

_____

_____

_____

Containers

31. *GSA approved:* Class _____ How many _____

32. *Open/closed signs:* _____

33. *Combinations changed by:* _____ On _____

34. *Combinations filed at:* _____

35. *Double check system:* _____

36. *Remarks:* _____

_____

_____

_____

Alarm Protection

If at least two appropriately cleared personnel are on duty 24 hours every day and have the capability of continuous audio or visual surveillance of the entire facility, the following is not required; however, it is suggested that it be completed for information purposes. Give manufacturer and model numbers in answering the following questions where applicable.

37. *Door protection:*

a. Alarm door switch _____

b. Television _____

c. Heat detector _____

d. Lacing _____

e. Capacitance _____

f. Other _____

38. *Window protection:*

a. Alarm tape _____

b. Switch _____

c. Capacitance _____

d. Television _____

e. Other _____

39. *Perimeter wall protection:*

a. Vibration detection _____

b. Lacing _____

c. Capacitance _____

d. Other _____

40. *Interior protection:* (within facility, below false ceiling)

a. Volumetric alarm system _____

b. Television _____

c. Other _____

41. *Ventilation and duct protection:*

a. Barriers _____

b. Acoustic baffles _____

c. Canvas, rubber, or transparent plastic vent connection joints _____

_____

d. Inspection ports _____

e. Breakwire alarms _____; Duct trap _____

f. Capacitance _____

g. Other _____

42. *Overhead protection:* (space above false ceiling)

a. Volumetric alarm system _____

b. Vibration detection _____

c. Alarm lacing _____

d. Other _____

43. *Perimeter (fence) protection:*

a. Fence alarm _____

b. Capacitance _____

c. Television _____

d. Guards and/or sentry dogs _____

44. *Line supervision protection:*

a. Inspection only, explain _____

b. Continuous conduit _____

c. Low security line supervision _____

d. High security line supervision _____

e. Other _____

45. *Guard response time for an alarm:* _____

When last tested _____

46. *Are all alarms operational?* _____

_____

47. *Is emergency/back-up power available for the alarm systems?*

Yes _____ No _____ How Long? _____

48. *Location of alarm annunciator panel:* _____

_____

49. *Is the alarm system equipped with the "REMOTE TEST" feature?* _____

_____

50. *If Ultra Sonics (volumetric alarms) are used, has the "oscillator" circuit been modified so as to create an alarm should component failure occur?* Yes, How? _____ No, Why? _____

51. *Is procedure established for periodic testing of alarms?* _____

_____

52. *When last tested:* _____ **By whom** _____

53. *Description of test methods:* _____

_____

_____

Telephone System

54. *Type of system installed:*

a. Switchboard _____ Type _____

b. Key system _____ Type _____

c. Conventional (one or two line instruments) _____

d. Other _____

55. *Are the key system and main frame located within the facility?* Yes _____ No _____ Answer the following:

a. Where is the main frame located? _____

_____

b. What type of security is afforded the main frame equipment room? _____

_____

c. Where is the key system located? _____

_____

d. What type of security is afforded the key system equipment? _____

_____

e. How are the telephone lines routed from the frame room to the facility or key system? _____

_____

_____

f. What type of security is afforded the telephone lines? _____

_____

56. *Number and type of instruments installed: (manufacturer, model number)* _____

_____

57. *Type of ringer unit used for each instrument:*

a. Non-resonant, give manufacturer and model number _____

_____

b. Light signal unit, describe _____

c. Other, describe _____

58. *Category of telephone security:*

a. Category I _____

b. Category II _____

c. Category III _____

d. Remarks _____

_____

59. *Is telephone equipped with "HOLD" feature?* Yes _____ No _____ Is handset equipped with:

a. WE type G-10F Push-to-operate _____

b. Other, describe by manufacturer, model number and mode of operation _____

_____

60. Remarks: _____

_____

_____

_____

Administration

61. *Routine destruction:*

a. How and where is waste stored; how often collected? _____

_____

b. Method of destruction _____

c. Nomenclature of disintegrator (if applicable) _____

d. By whom? _____

e. Are certificates of destruction completed and maintained? _____

_____

62. *Emergency destruction plan:*

a. Is it part of overall command or agency plan? _____

b. What priority is assigned to the sensitive compartmented information material? _____

_____

c. Is plan practical? _____

d. What type of devices are available for accomplishing the emergency destruction of material? _____

e. Make and model number of pulping or shredding equipment used (if applicable) _____

_____

f. Where are the emergency destruction sites located in relationship to the facility?

_____

63. *Char Force:*

a. Used to clean secure areas _____

b. Clearances _____

c. Security procedures in effect when char force is in the area _____

_____

64. *ADPS:*

a. What is the highest level of classified information processed?

C S TS SI TK Other (Specify) _____

b. If SCI is processed, has TEMPEST accreditation been granted in accordance with references e and f (yes) (no) and overall ADP system accreditation granted in accordance with DIAM 50-4 (yes) (no)?

65. *Local security situation:*

a. Is the facility commander being briefed by local counterintelligence personnel regarding the local counterintelligence situation? _____

_____

b. By whom? _____

c. How often? _____

66. *Remarks:* _____

_____

_____

_____

Intercom Systems

67. *Is an intercom system used?* No _____ Yes _____ Type _____

a. Telephone component feature (If this type, disregard following.) _____

_____

b. Separate system; give type of system _____

_____

68. *Are all stations within the facility?* Yes _____ No _____

If answer is no, give justification why station(s) must be outside of the facility and describe the measures used to protect the facility from technical penetrations by using the intercom lines routed to stations outside of the facility _____

_____

_____

_____

69. *Has the intercom sytem been tested by technicians during a technical survey?*
Yes _____ No _____ What were the findings, and have recommendations been complied with?
Yes _____ No _____ (If not, why?)

70. *Are there any disconnect or special security features installed?* No _____ Yes _____
Describe _____

_____

_____

71. *Remarks:* _____

_____

_____

_____

Sound Cover Systems

72. *Does the facility have a sound cover system installed?*

Yes _____ No _____ (If no, disregard the following.)

73. *What type of sound source is used to produce the sound cover for the systems?*

a. *Phonograph* _____

b. *Tape recorder* _____

c. *Other* _____

74. *How are the audio transmission lines routed from the system's amplifier to each speaker/enclosure and what type of cable is used for this purpose?*

a. Unshielded cable _____

b. Shielded cable _____

c. Electrical metalic tubing (EMT) (Conduit) _____

75. *Are all of the speakers/enclosures contained within the facility?* Yes _____ No _____

76. *Has the sound cover system been tested by technicians during a technical survey?*

Yes _____ No _____ What were the findings, and have recommendations been complied with? (If not, why? _____

_____

_____

77. *Remarks:* _____

_____

_____

_____

Electrical/Electromechanical Equipment

78. *Does the facility contain electrical/electromechanical equipment used to process sensitive compartmented information?* Yes _____ No _____ (If affirmative, complete the TEMPEST Security Checklist, enclosed with TCO/BCO DoD letter, "Sensitive Compartmented Information TEMPEST Policy and Guidance," 15 May 1979.

Unusual Security Vulnerabilities

79. ***Is the facility located in an area that is subject to burglarious attack and/or mob violence?***
Yes _____ No _____. If yes, describe nature of threat and additional security measures established to cope with this vulnerability. _____

_____

_____

_____

D. TEMPEST*

1. (U) Identification and location of organization submitting request.

2. (U) Floor plans of the building containing the SCI area which show the following:

a. The boundaries of the SCI area and SCI room numbers.

b. The classification level of the areas surrounding, above, and below the SCI area.

c. Areas where foreign nationals have access, including classified areas. Indicate whether areas are manned 24-hours a day by at least U.S. SECRET cleared personnel and under U.S. control.

d. Areas within facility where personnel with less than U.S. SECRET clearance can obtain access without being properly escorted or under continuous surveillance.

3. (U) Drawing showing:

a. Outline of building containing SCI area and its surrounding outside area, including roadways, loading zones, parking lots, etc.

b. If applicable, areas outside the building which are protected with approved alarm systems or which are under continuous surveillance by personnel with at least a U.S. SECRET clearance.

4. (U) Floor plan of SCI area showing:

a. Location and identity of electronic equipments by manufacturer and model number and, if applicable, the circuit with which the equipments are associated.

b. The classification level of information processed by each equipment.

c. Routing and identity of lines, cables, and other metallic conductors which leave the SCI area, including telephone, power, signal, and alarm lines, pipes, air conducting ducts, etc.

---

*Source: TCO/BCO DOD Letter, "Sensitive Compartmented Information TEMPEST Policy and Guidance (U)" CONFIDENTIAL, 15 May 1979.

d. Location of telephone instruments, telephone line filters, power line filters, signal ground points, etc.

5. (U) Will signal lines carrying unencrypted SCI information be routed into areas of lower classification or into uncontrolled areas? If so, describe TEMPEST and physical security protective measures outside of SCIF.

6. (U) Will SCI be transmitted outside the SCIF? If so, identify user, building, and room number of distant location for each circuit. If circuit goes directly to an AUTODIN Switching Center (ASC), just identify the ASC.

7. (U) Will both SCI and collateral information be processed electronically within the SCI areas? If so, is the signal line distribution installed in accordance with DoD Directive C-5030-58-M (pages 17-19)?

8. (U) What percentages of SCI, TS, S, C, U are processed by each equipment? Indicate total number of hours/week each equipment is used.

9. (U) Identify all electronic equipments and wirelines that are located within six feet of SCI equipment and SCI signal lines.

10. (U) Do cables carrying SCI information to, from, and between equipments have at least one overall non-ferrous metallic shield? If no, describe. Are they in metallic conduit or ducts?

11. (U) Reference Figures 1, 2, and 3. Do all telephone cables in the SCI area have at least one overall non-ferrous metallic shield? Are they in metallic conduit or ducts? Are they filtered before leaving (a) the SCI area or (b) lesser facility controlled area? If answer to (b) is yes, describe. Are filters grounded to a low impedance ground within the controlled area? Is maximum separation maintained between lines to and from filters, e.g., not grouped together? Are signal cables separated from telephone lines?

12. (U) Do pipes and air conditioning ducts leaving the SCI area have non-conductive sections at their points of egress from (a) the SCIF or (b) lesser facility controlled area? If answer to (b) is yes, describe.

13. (U) Are the SCI equipments installed within an RF-shielded room? If so, provide manufacturer's name, model number, and attenuation characteristics, if available.

14. (U) Has a RED/BLACK inspection been performed to determine compliance of the facility with RED/BLACK engineering criteria of MIL-HDBK-232? If so, provide copy of inspection report and describe corrective measures implemented if discrepancies were identified.

15. (U) Has an instrumented TEMPEST survey (TEMPEST Test) been performed? If not, has a test been scheduled? If so, were emanations detected outside (a) the SCI area, (b) areas under continuous (direct or CCTV) surveillance by at least SECRET cleared personnel or where protective measures (alarm systems) are used (refer to paragraph 4. of Policy and Guidance on Control of Compromising Emanations). Describe corrective measures if discrepancies were identified. Forward copy of test report.

E. ADP SECURITY

A. **HARDWARE** *

	YES	NO	COMMENTS
1. Utilization:			
a. Do you monitor your operations for compliance with schedules?	------	----	----------
b. Do you correlate meter hours with utilization hours?	------	----	----------
c. Do you monitor scheduled maintenance activities to ensure proper reliability and hardware performance?	------	----	----------
d. Do you verify all periods of down time?	------	----	----------
e. Do you check "end meter" with "begin meter" readings each morning for unexplained gaps?	------	----	----------
f. Do you check all incoming work against an authorized user list?	------	----	----------
g. Do you spot-check output for possible misuse of system	------	----	----------
h. Do you have an updated distribution system to prevent an unauthorized person from receiving a confidential report?	------	----	----------
2. Communications Security:			
a. Do all communication links between remote terminal areas and the central computer facility meet the requirements for the transmission of the higher classification and for all categories of data which are contained in the system?	------	----	----------
b. Are all remote terminals uniquely identified?	------	----	----------
c. Are dial-up terminals disabled from connection to the central computer facility during classified processing periods?	------	----	----------
3. Emanations Security:			
a. Has the facility been evaluated in accordance with applicable TEMPEST procedures to determine risk?	------	----	----------
b. Has all installed ADPE been TEMPEST tested?	------	----	----------
c. Has ADPE which does not meet TEMPEST requirements been provided filtered power, if necessary?	------	----	----------
d. Are all changes, repairs, and modifications to TEMPEST modified ADPE controlled so that the equipment emanations characteristics are not altered?	------	----	----------
4. Erase and Declassification Procedures:			
a. Is each memory location used for the storage of classified data overwritten when it is no longer required before reuse, or before the content of the location may be read?	------	----	----------
b. Are the necessary programs, equipment, and procedures for declassifying any and all ADP equipment used for the processing or storage of classified data on site?	------	----	----------

*Sources: DoD 5200.1-R, DoD 5200.28, MIL-HDBK-232, AR 18-1, AR 530-4

		YES	NO	COMMENTS
5.	Magnetic Tapes and Disks:			
	a. Does your tape and disk accountability procedure cover:			
	(1) Frequency of use?	------	----	----------
	(2) Frequency of cleaning?	------	----	----------
	(3) Authorized user?	------	----	----------
	b. Are magnetic tapes and disks filed in an orderly manner?	------	--	----------
	c. Are tapes cleaned on a regular basis (once each 10 uses is recommended)?	------	----	----------
	d. Do you check and clean your disk packs or have it done by contract?	------	----	----------
	e. Are tapes kept in their containers except when in use?	------	----	----------
	f. Are tapes stored vertically?	------	----	----------
	g. Are tape utilization records maintained?	------	----	----------
	h. Are tape containers cleaned periodically?	------	----	----------
	i. Are tape heads cleaned every shift?	------	----	----------
	j. Do you sample test your tapes periodically for drop-outs, to determine the general condition of your tape library?	------	----	----------
	k. Do you strip frayed leader regularly?	------	----	----------
	l. Have you investigated the possibility of a tape rehabilitation or recertification program?	------	----	----------
	m. Is your tape library located in an area secure from explosion or other dangers?	------	----	----------
	n. Do you use storage vaults specifically designed for magnetic media for critical tape files?	------	----	----------
	o. Have you considered magnetic detection equipment to preclude the presence of a magnet near your tapes and disks?	------	----	----------
	p. Do you provide similar protection for your tape files while they are in transit to a backup site, etc.?	------	----	----------
	q. Are ADP products marked with:			
	(1) Date of creation?	------	----	----------
	(2) Highest classification of any information contained in in the product?	------	----	----------
	(3) Downgrading or exemption instructions when placed in permanent files?	------	----	----------
	(4) A unique identifier?	------	----	----------
	(5) The classification of the system's environment when the product was produced if the assigned classification cannot be immediately verified by the customer?	------	----	----------

	YES	NO	COMMENTS
r. Are all ADP storage devices marked with:	------	----	----------
(1) The overall security classification which meets the highest classification of any information stored on the device?	------	----	----------
(2) Special access restrictions?	------	----	----------
(3) A permanently assigned identification/code number?	------	----	----------
(4) A color code?	------	----	----------

B. SOFTWARE SECURITY *

1. Physical Security:

a. Are the essential programs, software systems, and associated documentation in your Program Library located in a locked vault or secured area?	------	----	----------
b. Have you provided backup files at a secondary location for both the programs and the associated documentation?	------	----	----------

2. Access Restrictions:

a. Have you restricted access to the essential programs and software systems on a need-to-know basis in the prime and backup areas?	------	----	----------
b. Do you employ a multilevel access control to your data files?	------	----	----------
(1) By various levels of security classification?	------	----	----------
(2) By various breakdowns within a file, i.e., by block, record, field, and characters?	------	----	----------
(3) By read only, write only, update, etc.?	------	----	----------
c. Do you perform periodic checks to validate the security software utilities and tables of access codes?	------	----	----------
d. If you employ remote access to online data bases, do you employ techniques to prevent more than one user updating files at any given time?	------	----	----------

3. Remote Terminals:

a. Do you employ keyword or password protection?	------	----	----------
(1) If so, do you change keywords and passwords semi-annually (annually)?	------	----	----------
b. Do you employ software scrambling techniques during transmission of vital data?	------	----	----------
c. Do you employ hardware cryptographic devices during transmission of vital data?	------	----	----------
d. Do you restrict terminal users to higher level languages such as COBOL, FORTRAN, and PL/1, to prevent their access to machine language coding (which can be used by a knowledgeable systems programer to over-			

*Sources: DoD 5200.28, DoD 5200.28-M

	YES	NO	COMMENTS
ride or alter software such as operating systems, security utilities, tables, etc.)?	------	----	----------
4. Operating Systems:			
a. Do your operating systems have built in protection to prevent the bypassing of security utilities and the unauthorized access to data bases by a knowledgeable programer familiar with the system?	------	----	----------
b. Are memory bounds tested following maintenance, initial program load, and each restart?	------	----	----------
c. Can your own software systems technologists be depended upon not to circumvent the normal access procedures by use of a special coding thus violating the integrity of the system?	------	----	----------
d. Are all modifications to the operating system verified by by the Security Officer or personnel designated by him?	------	----	----------
e. Is a record of all operating system modifications maintained until at least the next software release?	------	----	----------
5. Application Programs:			
a. Are well designed restart and recovery procedures incorporated and utilized?	------	----	----------
b. Do your restart procedures properly handle the more complex requirements presented by files that are processed in random rather than sequential order?	------	----	----------
c. Are programing changes and maintenance well controlled and documented?	------	----	----------
d. Do you employ diagnostic and test routines to validate outputs from critical reporting systems?	------	----	----------
6. Threat Monitoring:			
a. Do you maintain a monitor log of those who access data banks or any sensitive files?	------	----	----------
b. Do you use a software security routine to monitor attempts to access sensitive files by unauthorized users?	------	----	----------
(1) Does this routine notify the operator via the on-line console?	------	----	----------
(2) Does this routine provide a record of all such attempts via a printout at day's end?	------	----	----------
c. Does your organization use the data obtained above to develop patterns which can help to track down possible suspects who misuse or have unauthorized access to vital data records?	------	----	----------
d. Are all security incidents investigated to determine their cause and where possible, the corrective action to be taken?	------	----	----------

	YES	NO	COMMENTS
e. Is a formal investigation in accordance with DOD Regulation 5200.1-R conducted whenever a compromise or suspected compromise is the result of the security incident?	------	----	----------
C. SERVICE PERSONNEL			
1. In-House:			
a. Do you control access to vital areas for custodial, electrical, and other in-house maintenance personnel?	------	----	----------
b. Do you provide special escorts for maintenance personnel who are not appropriately cleared?	------	----	----------
2. Vendor:			
a. Do you have a list of each vendor's authorized service and systems support personnel?	------	----	----------
b. Do you insist on positive identification?	------	----	----------
c. Do you supervise their activities to ensure that they don't compromise your security?	------	----	----------
d. Do you insist that vendors verify that they have performed a background check on their personnel?	------	----	----------
D. FILES			
1. On-Line and Off-Line Program Files:			
a. Are the duplicate files stored in a separate building from the originals?	------	----	----------
b. Have you considered the merits of leasing underground storage space from a reputable vital records concern?	------	----	----------
c. Do you store programs in low fire hazard containers?	------	----	----------
d. Do you have a current inventory of such files?	------	----	----------
e. Have you held a "dry run" in the past 3 months to test the ease and accuracy of your file backup system?	------	----	----------
f. Are program changes controlled and recorded?	------	----	----------
g. Are changes made only to a reproduced version of the original program file with the original left intact?	------	----	----------
h. Do you maintain a record of items withdrawn from production file area?	------	----	----------
i. Does Computer Operations review systems documentation for compliance with operational standards?	------	----	----------
j. Do you maintain any type of backup of source data for programs under development?	------	----	----------
k. Are programs classified according to a predetermined classification policy?	------	----	----------

	YES	NO	COMMENTS
2. Documentation:			
a. Do you have documentation standards which include:			
(1) Logic or flow charts?	------	----	----------
(2) Current listing?	------	----	----------
(3) Input and Output formats?	------	----	----------
(4) Output samples?	------	----	----------
(5) User documentation?	------	----	----------
(6) Copies of test data?	------	----	----------
(7) Adequate explanation of codes, tables, calculations, etc.?	------	----	----------
(8) Explanation of error messages?	------	----	----------
(9) Rejected record procedures?	------	----	----------
(10) Explanation of halts?	------	----	----------
(11) File sequence description?	------	----	----------
(12) Control and balancing instructions?	------	----	----------
b. Do you maintain duplicates of all documentation?	------	----	----------
c. Is the duplicate filed in a separate building from the original?	------	----	----------
d. Do you utilize low fire hazard storage equipment for documentation?	------	----	----------
e. Do you inventory this file at least annually?	------	----	----------
f. Do you review your documentation backup periodically to ensure its current applicability?	------	----	----------
g. Are changes in programs and documentation coordinated and approved by the cognizant areas?	------	----	----------
h. Are changes reviewed by the internal auditor?	------	----	----------
i. Does Computer Operations review systems documentation for compliance with operational standards?	------	----	----------
3. Data Files:			
a. Is the retention cycle for the data files documented for each application?	------	----	----------
b. Does the user review this procedure regularly for compliance?	------	----	----------
c. Are all data files maintained within and under the control of the computer complex rather than user?	------	----	----------
d. Are files classified in terms of degree of sensitivity and value to the organization?	------	----	----------
e. Are files (tape, disk, or card) kept in an area other than the computer room?	------	----	----------

	YES	NO	COMMENTS
f. Is this area fire-protected?	------	----	----------
g. Is access specifically controlled?	------	----	----------
h. Do you use special low fire hazard storage containers for critical files?	------	----	----------
i. Is your program for source document retention coordinated with your file reconstruction procedures?	------	----	----------
j. Do you "dry run" your data file security system periodically to ensure compliance with standard procedure?	------	----	----------
k. Do you know the relative value of a given program application or file?	------	----	----------
l. Do you understand and comply with the legal requirements for file retention?	------	----	----------
m. Do you educate the user to participate effectively in a file classification program?	------	----	----------

E. INTERNAL AUDIT CONTROLS

1. Does an overall audit control philosophy exist relatingto computer systems concerned with assets?	------	----	----------
2. Are computer usage and production controls employed?	------	----	----------
3. Is user input controlled to ensure receipt of all input data?	------	----	----------
4. Is output monitored to ensure compliance with standards?	------	----	----------
5. Do error reporting and follow-up procedures exist?	------	----	----------
6. Does a quality control exist to verify proper execution of reports?	------	----	----------
7. Are program changes controlled?	------	----	----------
8. Are all options of all programs tested?	------	----	----------
9. Are conversions controlled to ensure continuity?	------	----	----------
10. Does the installation ensure separation of duties?	------	----	----------
11. Is the installation adequately protected against intrusion?	------	----	----------
12. Does backup exist for programs and files?	------	----	----------
13. Does backup exist for hardware?	------	----	----------
14. Are the systems auditable?	------	----	----------
15. Does the auditor get involved during the system design phase?	------	----	----------

F. TIME-RESOURCE SHARING

(i.e., the concurrent use of any system by two or more users—includes time sharing, multiprocessing, multiprograming, etc.)

1. Are remote terminals available only to selected individuals?.	------	----	----------
2. Is access to terminal controlled by:			

	YES	NO	COMMENTS
a. Locked doors?	------	----	----------
b. Posted guards?	------	----	----------
c. Other restraints?	------	----	----------
3. Is the location of the terminal such that each user's privacy is ensured?	------	----	----------
4. Do you have an absolute control of portable terminals to prevent their theft and misuse?	------	----	----------
5. Do you utilize "passwords" to identify a specific terminal and a specific user?	------	----	----------
6. Is the password protection system really tamperproof?	------	----	----------
7. Is the interval at which passwords are changed appropriate to the security requirements?	------	----	----------
8. Is the password combined with physical keys or access badges?	------	----	----------
9. Does the system software restrict a given individual to specific data files only?	------	----	----------
10. Is the right to add, delete, or modify files limited by software controls?	------	----	----------
11. Is access to the "keyword" and "lockword" files restricted?	------	----	----------
12. Does the system maintain accurate records of all activity against each data file?	------	----	----------
13. Are security-override procedures classified at the highest level and the use of override closely monitored?	------	----	----------
14. Are scramblers or other cryptographic techniques utilized as appropriate?	------	----	----------
15. Is the time-resource sharing security system monitored and reviewed?	------	----	----------
16. Is program debugging of the security system closely monitored and controlled?	------	----	----------
17. Do you have software protection of online operating systems/applications programs?	------	----	----------

G. CONTINGENCY PLAN

1. Backup Facilities:			
a. Do you have a backup computer available?	------	----	----------
(1) If yes, is it in:			
(a) The same room? (not good)	------	----	----------
(b) A different room—same building? (better)	------	----	----------
(c) A separate location? (best)	------	----	----------
(2) Can it handle your workload?	------	----	----------

	YES	NO	COMMENTS
b. If not, do you have access to another computer?	------	----	----------
(1) Contractual agreement?	------	----	----------
(2) Test at least quarterly?	------	----	----------
(3) Does the installation take computer security seriously?	------	----	----------
(4) Can it handle your workload?			
c. Do you have an implementation plan for use of backup installation?	------	----	----------
d. Do you test and review it periodically?	------	----	----------
e. Do you have a regular maintenance schedule?	------	----	----------
f. Do you monitor it for compliance?	------	----	----------
g. Does the vendor stock spare parts locally?	------	----	----------
2. Do you have a written contingency plan covering:			
a. Who is responsible for each functional area?	------	----	----------
b. A detailed notification procedure clearly specifying—"Who calls whom?"	------	----	----------
(1) Management?	------	----	----------
(2) Emergency crews?	------	----	----------
(3) Users?	------	----	----------
(4) Backup sites?	------	----	----------
(5) Service personnel?	------	----	----------
(6) Facilities personnel?	------	----	----------
c. Criteria for determining extent of disruption?	------	----	----------
d. The responsibility for retaining source documents and/or data files for each application?	------	----	----------
e. Identification of backup installations?	------	----	----------
f. Destruction or safeguarding of classified material in the central computer facility in the event the facility must be evacuated?	------	----	----------
g. Items such as:			
(1) Purchase or lease of new or temporary computer equipment?	------	----	----------
(2) Acquisition of air conditioning equipment?	------	----	----------
(3) Purchase of computer time/services?	------	----	----------
(4) Acquisition of additional manpower?	------	----	----------
(5) Acquisition of furnishings, cabinets, etc.?	------	----	----------
(6) Acquisition of replacement tapes/diskpacks?	------	----	----------
(7) Alternate site preparation?	------	----	----------

	YES	NO	COMMENTS
(8) Travel accommodations?	------	----	----------
(9) Orderly transportation of computer jobs, personnel, and related materials?	------	----	----------
(10) Duplication of backup files?	------	----	----------
(11) Continuing security in contingency mode?	------	----	----------
h. Do you have a contingency training program for all ADP personnel?	------	----	----------

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX G

ACCESS NOMINATION FORM (U)

THIS PAGE INTENTIONALLY LEFT BLANK

(U) This appendix provides the format for requesting access to CHOSUN facilities and/or the CHOSUN network. The incomplete form is UNCLASSIFIED. The completed form will be classified SECRET.

UNCLASSIFIED

CLASSIFICATION

PROJECT CHOSUN ACCESS NOMINATION FORM

1 DATE

2 TO

CHOSUN NETWORK SECURITY OFFICER

3 FROM

REQUESTING AGENCY

4 NOMINEE IDENTIFICATION

FULL NAME | RANK/GRADE | DATE OF BIRTH

PLACE OF BIRTH | SOCIAL SECURITY NUMBER

ADDRESS OF AGENCY/ORGANIZATION ASSIGNED | POSITION

TELEPHONE NUMBER | SCHEDULED DEPARTURE/REASSIGNMENT DATE

5 CLEARANCE/INVESTIGATIVE DATA

LEVEL HELD | SCI ACCESS | INVESTIGATIVE AGENCY

DATE GRANTED | TYPE OF INVESTIGATION

AGENCY SECURITY OFFICER APPROVAL | (SIGNATURE CERTIFIES COMPLIANCE WITH CLEARANCE/INVESTIGATIVE REQUIREMENTS SPECIFIED IN CHOSUN NETWORK SECURITY MANUAL)

6 JUSTIFICATION FOR ACCESS

SPECIFY NODES TO BE ACCESSED, REASON FOR ACCESS, NEED-TO-KNOW, TYPE OF ACCESS (I.E., FACILITY ONLY OR NETWORK)

PERIOD OF ACCESS (SPECIFY DATE(s))

NISSO/HISSO/PMO SIGNATURE | DATE OF SIGNATURE

AGENCY SIGNATURE APPROVAL | POSITION OF APPROVING AGENT

DATE OF APPROVAL

7 ACCESS AUTHORIZATION

NSO SIGNATURE | APPROVAL/DISAPPROVAL | DATE

DAA SIGNATURE | APPROVAL/DISAPPROVAL | DATE

COMMENTS

CLASSIFICATION

UNCLASSIFIED

APPENDIX H

STATEMENT OF WORK FOR AN RF-SHIELDED ENCLOSURE (U)

Classified by: NSDD-95
Declassify on: OADR

(U) NOTE: This Outline Statement of Work is classified CONFIDENTIAL. When detailed site-unique information is added to Attachments A, D, E, G, I, and J and the document is associated with a specific Project CHOSUN site, the Final Statement of Work must be classified a minimum of SECRET, as determined by the result of a review by cognizant authority.

THIS PAGE INTENTIONALLY LEFT BLANK

PREFACE

(C) This outline document provides a mechanism for the procurement of a Project CHOSUN standard RF-shielded enclosure in which to house a node video console and a node digital data console. Essentially, the document complies with NSA's NACSEM 5204, Appendix B (NSA Specification No. 65-6, which provides 100 dB of electromagnetic attenuation) amended to include: 45 dB worth of acoustic treatment; 18 to 24 inches of clear space around and over the RF-shielded room; a minimum of 4 inches of clear space under the enclosure; and special treatment of the parent room.

THIS PAGE INTENTIONALLY LEFT BLANK

CONTENTS

ATTACHMENTS

SECTION 1. INTRODUCTION (U)

1.1 Background (U)

(C) One safeguard the U.S. Government uses to protect its sensitive information from being electrically compromised is conducting classified meetings and discussions in permanent electromagnetic shielded enclosures. Therefore, offerors are requested to submit proposals for the design, fabrication and installation of an RF-shielded enclosure as identified in attachment A hereto. Assembly and installation of this enclosure shall be at a Government facility in the Washington, D.C., metropolitan area. The exact location will be identified upon date of contract award, or sooner if deemed necessary by the Government.

1.2 Scope of Work (U)

(U) The Contractor shall provide the qualified personnel, facilities and materials necessary to design, fabricate and install an RF-shielded enclosure as denoted herein, in accordance with the attached general specifications which are hereby incorporated by reference and made a part hereof.

(U) This Statement of Work, with its attachments, covers the design, fabrication and installation of the above-mentioned RF-shielded enclosures, hereinafter referred to as "enclosure."

SECTION 2. GENERAL REQUIREMENTS (U)

2.1 General (U)

(U) The enclosure shall be assembled by a firm regularly engaged in the manufacturing of RF-shielded enclosures and must have built similar enclosures of at least the size specified in attachment A. No prototype or nonstandard items will be used. All equipment and devices must be in common use and have spare parts readily available.

2.1.1 (U) RF-Shielded Enclosure. The Contractor shall furnish a turn-key shielded enclosure designed, built, and assembled at Government facilities or identified by the Contracting Officer and in conformance with NSA Specification No. 65-6, including Heating-Ventilation-Air Conditioning (HVAC), electrical, plumbing, fire detection, and architecturally sound systems.

(U) The RF-shielded enclosure shall be built and tested strictly to the requirements of NSA Specificiation No. 65-6 (Appendix B of NACSEM 5204), unless specified exemptions or changes are made within

this Statement of Work. Where the above NSA Specification does not give specific direction on a particular construction or testing problem, the Contractor shall propose one or more possible solutions to the Contracting Officer's Technical Representative (COTR) for his approval or selection prior to implementation. Discrepancies noted by the Contractor between the NSA Specification cited above, other specifications to be followed in part (such as NACSIM 5203 or those listed in Section 4. herein) or any Government furnished or approved drawings shall be promptly brought to the attention of the COTR for clarification and resolution.

2.2 (U) The enclosure(s) shall meet (or exceed) the electromagnetic attenuation requirements as described in attachment B, hereinafter referred to as "attenuation requirement."

2.3 (U) The enclosure(s) shall continue to meet (or exceed) the attenuation requirements for a period of three (3) years after initial field acceptance without requiring major maintenance (i.e., retightening of bolts, screws).

2.4 (U) The enclosure(s) shall meet (or exceed) the acoustic attenuation requirement as described in attachment C.

2.5 (U) Whenever possible, the enclosure(s) shall have interchangeable wall panels to permit the relocation of panels containing the door, power line filters, signal line penetrations, and air conditioning and ventilation penetrations during installation while still maintaining all the requirements of this Statement of Work (SOW).

2.6 (U) The enclosure(s) shall be capable of being increased or decreased in length and/or width, at a later date, by the addition or removal of one or more of the RF panels while still maintaining all the requirements of this specification.

2.7 (U) The enclosure(s) shall be capable of disassembly and subsequent reassembly, at a later date, while still maintaining all the requirements of this specification.

SECTION 3. ASSEMBLY AND INSTALLATION (U)

(U) Installation of the enclosure(s) will be at a later date at a location somewhere within the Washington, D.C., metropolitan area as specified by the Contracting Officer. The Contractor shall provide installation personnel within ten (10) days after delivery of the enclosure.

SECTION 4. APPLICABLE PUBLICATIONS (U)

4.1 (U) The following standards of the latest addition in effect on the date of invitation for bid form a part of this specification to the extent specified herein. The requirements of this specification, its attachments and supplements will prevail in the event of conflict with any of the below-mentioned publications.

4.2 Department of Defense, National Security Agency (U)

a. (U) NACSEM 5203	Guildelines for Facility Design and Red/Black Installation
b. (U) NACSEM 5204	Shielded Enclosures
c. (U) NSA Specification No. 65-6	National Security Agency Specification for RF-Shielded Enclosures for Communications Equipment: General Specification (Appendix B of NACSEM 5204)

4.3 Military Standards (U)

a. (U) MIL-STD-220A	Method of Insertion-Loss Measurement
b. (U) MIL-STD-285	Attenuation Measurement for Enclosures, Electromagnetic Shielding, for Electronic Test Purposes, Method of
c. (U) MIL-F-15733	Filters, Radio Interference, General Specification for

4.4 American Standards (U)

a. (U) American National Standards Institute	(All Applicable Publications)
b. (U) National Electrical Code	

SECTION 5. DRAWINGS, INSTRUCTIONS, AND REPORTS (U)

5.1 Preliminary Drawings (U)

(U) Four (4) sets or preliminary drawings (not less than 24" x 36") of the proposed enclosure, to include one set of sepias, shall be submitted to the Contracting Officer or his representative within

twenty (20) days after award of the contract. They shall include an architectural drawing showing the dimensions of the enclosure and external features such as power line filters, floor and ceiling supports systems, signal line penetrations, air conditioning and ventilation penetrations, door and door swing area requirements, and any other features which may require modification to the original enclosure design and/or the parent room.

5.2 Final Drawings (U)

(U) Two (2) complete sets of final drawings shall be included with the shipment of each enclosure. One (1) set of not less than 24-inch x 36-inch mylar sepias must be provided to the Contracting Officer or his representative not less than fifteen (15) days prior to shipment of the enclosure. Sepias must be of highest quality and produce clearly detailed copies. Drawings will not be reduced in size from originals. The final drawings shall incorporate all revisions, additions, deletions, and/or corrections resulting from the review of the preliminary drawings. In addition, they will include, for each enclosure:

a. (U) An architectural drawing showing the dimensions of the enclosure and external features such as systems, signal line penetrations, air conditioning and ventilation penetration, door and door swing area requirements.

b. (U) An architectural drawing of the interior finish.

c. (U) Detail drawings of the RF panels; floor and ceiling support systems; access openings, power, signal, air conditioning and ventilation penetrations; and lighting layout.

d. (U) Cross-sectional drawing of the walls, floor, and ceiling including the floor and ceiling support systems and interior finish.

e. (U) Cross-sectional drawings of the access opening.

f. (U) Electrical schematic diagrams and connection drawings of the power line filters, power distribution panel(s), access opening alarm, and lighting.

g. (U) A complete set of installation instructions describing in detail the step-by-step procedure for installing the entire enclosure and auxiliary components.

h. (U) The original manufacturer's (not Contractor's) descriptive brochure or service manual for each auxiliary device. (The Contractor's brochure or service manual for auxiliary devices will be accepted only when no manufacturer's brochure or service manual exists.) Xerox-type copies are not acceptable.

SECTION 6. MATERIAL (U)

6.1 General (U)

(C) All materials used in the construction of the enclosure shall be new, of current manufacture, and of a high grade, free from all defects and imperfections. Workmanship shall be in acccordance with good modern industrial practices. Should a definite material not be specified, a material shall be used which will meet the requirements of this specification and will be in agreement with good engineering practices.

6.2 Substitution of Parts and Materials (U)

(U) If the Contractor desires to substitute another part or material (1) where the specifications and approved drawings require a specific item, or (2) where a particular part or materials have been previously approved for use, he shall notify the Contracting Officer immediately (by telephone) and submit a written statement describing the proposed substitution and the reason therefor. Along with the statement, he shall submit evidence that such a substitution is at least the equal of the part of material specified or previously approved. At the discretion of the Contracting Officer, samples may be required which will demonstrate by testing the suitability of the proposed substitution.

6.3 Mechanical (U)

6.3.1 (C) Enclosure Size. The size of the enclosure shall be specified in the specification applicable to each enclosure (attachment D). The minimum inside vertical dimension of the enclosure will be no less than nine feet, with approximately one foot used for a raised floor and six inches utilized for a hung ceiling. The adequacy of the remaining seven feet, six inches for the node operational area will be determined by the Government and the Project CHOSUN prime contractor.

6.3.2 (U) Parent Room Dimensions. The parent room dimensions shall be specified in the specification applicable to each enclosure (attachment E).

6.3.3 (U) Enclosure Weight. The gross weight of the enclosure shall not exceed 80 pounds/square foot (as averaged over the floor area occupied by the enclosure).

6.3.4 (U) RF Panels. The RF panels shall be fabricated from zinc-coated steel, laminated to both sides of exterior-grade plywood or 3/4" wood particle board. The combined thickness (gauge) of the steel shall be sufficient to meet (or exceed) the attenuation requirements. Uniform panel thickness shall be ensured so that the mechanical joints form a positive, flat contact, thereby producing a tight RF seal between every mating surface. Contact between dissimilar metals shall be avoided to prevent galvanic action.

6.3.5 (U) Panel Size. The RF panels shall be no greater than 96 inches in length to 48 inches in width unless otherwise specified.

6.3.6 (U) Joints Between Panels. The framing (or clamping) system shall be fabricated from not less that 1/8-inch thick, zinc-coated, structural steel. The selection of material and its configuration shall provide the rigidity, elasticity and hardness necessary to ensure proper structural strength and RF-tight joints without need for RF gasketing, foil, caulking, knurling, welding, or soldering. Clamping pressure shall be applied to all seams by cadmium-plated, (no less than 1/4-inch) self-threading or machine, phillips-head or hex-head screws, placed on maximum 4-inch centers capable of proper and uniform torqueing to assure maximum metal-to-metal conformity and an RF-tight joint. Contact between dissimilar metals shall be avoided to prevent galvanic action. The framing (or clamping) system shall be designed so that installation can be accomplished entirely from inside the enclosure. The framing (or clamping) system shall meet (or exceed) and maintain the attenuation requirements without maintenance (i.e., retightening of bolts, screws) for a minimum or three (3) years.

6.3.7 (C) Under-Structure (Floor Support System). Supporting elements between the enclosure and the parent room floor shall be incorporated in the enclosure design. This system shall use transparent lucite and rubber blocks to elevate the enclosure no less than 2 inches and no more than 18 inches (unless otherwise specified) to provide unobstructed surveillance of the area between the underside of the enclosure and the floor of the parent room.

6.3.8 (U) Structural Requirements

6.3.8.1 (U) Floor Loading. The floor support structure shall be designed to carry an average floor load of 80 pounds per square foot with a miximum point load of 175 pound per square foot over a 4-square-foot area.

6.3.8.2 (U) Deflection

6.3.8.2.1 (U) Walls. A static load of 75 pounds applied with normal pressure to the wall surface at any point shall not cause a deflection exceeding 1/250th of the span between supports.

6.3.8.2.2 (U) Ceiling. Deflection shall not exceed 1/480th of the span.

6.3.8.3 (U) Structural Support Beams. Structural support beams may be employed (on the outside of the enclosure only) provided the outside dimensions (length, width, and height specified in the Supplemental Data) are not exceeded. No parent room-to-enclosure ceiling supports shall be used unless specified.

6.3.9 (U) Assembly. The complete enclosure (i.e., RF panels, framing system, structural beams, under-structure) shall be capable of assembly on site without welding or soldering.

6.3.10 (U) Access Opening. Will consist of an entrance vestibule. The entrance vestibule, which will be the same performance and sound attenuation requirements as the enclosure, will be equipped with two interlocking electromagnetic door systems, Ray Proof Model RCM-8CM-85G-80 (or equivalent), to maintain shielding or the enclosure at all times. The outer door will have a Sergeant and Greenleaf Codetronics cipher lock Model 8419 for restricted personnel access to the room. Both doors will have special audio treatment to meet the attenuation requirements of attachment C. Operation of the door latching/unlatching mechanism and the overhead door actuator is through a series of microswitch contacts and actuator buttons or floor mats which control an electric motor drive of the latching mechanism and then the automatic door actuator. An electrical safety mat is provided on the swinging side of the door to instantaneously stop the opening or closing operation should anyone be in danger of being struck by the moving door leaf. The operation of the door is protected by means of a complete manual override capability. It must be possible to open the door from either side, in the event of a failure, such as loss of mechanical power, by means of an emergency manual mechanism. Doors shall be electrically interlocked to prevent simultaneous opening of both doors.

6.3.11 (C) Interior

6.3.11.1 (U) Floors. Masonite (or equivalent) shall be installed flush with the RF floor clamps. All RF floor clamps shall be secured by utilizing counter-sunk flat-head screws. A raised floor

of approximately one foot in height shall be installed. The floor covering shall be commercial grade carpet (color selection by customer).

6.3.11.2 (C) Walls. The interior walls shall be constructed of 5/8-inch sheet rock, attached by metal furring studs on 16-inch centers with door and ceiling tracks. Attached to this wall will be Armstrong Soundsoak 85, 1-inch-thick wall panels (a sample of available colors to be provided to customer for selection prior to ordering and installation.) Colors should be limited in range to ensure high color temperature for video camera signals. A soft blue or soft green is preferred, at least from the chair rail molding up. A 4-inch vinyl base molding will be provided at the base of the wall (color coordinated in the wall). See attachment F regarding Armstrong Soundsoak 85.

6.3.11.3 (C) Ceiling. The ceiling shall be constructed of 5/8-inch sheet rock attached by metal furring studs on 16-inch centers. A hung ceiling of approximately six inches in depth will be installed equipped with acoustical ceiling tile.

6.3.12 (U) Service Penetrations. The quantity, type and location of service penetrations will be as specified in attachment G.

6.3.13 (U) Air Conditioning Requirements. See attachment J.

6.4 Electrical (U)

6.4.1 (U) Power Line Filters. Specifications for the power line filters are provided in attachment H.

6.4.2 (U) Electrical. Specifications for the electrical distribution equipment and material are provided in attachment I.

6.4.3 (U) Grounding. The enclosure shall have a single point ground and be electrically isolated from any building ground systems or potential current-carrying material. Internal wiring shall have an isolated neutral, and a common grounding terminal will be provided on the external surface of the enclosure adjacent to the power penetrations.

6.4.4 (U) Lighting. Interior lighting shall consist of low profile, incandescent round-shaped ceiling fixtures (3-100W/nominal size of 15 1/2-inch diameter x 6-inch with nominal output of 4800 lumens). Light fixtures are to be surface mounted to acoustical tile. Lighting needs to be diffused for video operation and provide high color temperature. Light switches shall be provided and located near the entrance doorway. Each switch that controls

overhead lighting shall be equipped with a suitable dimmer switch. NOTE: If flourescent lamps are employed, they must be specially designed for use in a TEMPEST environment.

6.5 Fire Detection System (U)

6.5.1 (U) A fire detection system/smoke and ionization detector system shall be installed within the shielded enclosure. If a fire detector is activated, a bell or other audible warning device shall sound and a light shall illuminate within the enclosure and at a location (to be determined) outside the enclosure. Such outside location shall be in either the parent room or in close proximity thereto.

6.5.2 (U) The fire detection system will be provided and installed by the Contractor. The Contractor shall provide all conduit and wiring required to connect this system. Shielded wiring shall be used to connect the smoke and ionization detectors with the control circuits. Wiring shall be tagged for proper identification. All penetrations of the shield shall maintain the RF integrity of the enclosure.

SECTION 7. INSTALLERS (U)

(U) Installation of the enclosure as detailed herein shall be conducted by expert field technicians/representatives with Department of Defense national security clearances, minimum level of SECRET.

SECTION 8. INSPECTION AND MATERIAL TESTS (U)

8.1 Monitoring Inspections (U)

(U) During the design and fabrication phase of the enclosure(s), the Government reserves the right to conduct monitoring inspections at the Contractor's plant. It will be the responsibility of the Contractor to advise the Contracting Office of the details where deviations from the Statement of Work, its attachments or applicable specifications to each enclosure exist.

8.2 Material Inspections (U)

(U) After the enclosure has been fabricated, a material inspection may be made by the Contracting Officer or the COTR at the Contractor's plant to facilitate payment. This in no way relieves the Contractor of his resonsibility to provide any parts or material which may be missing at the time the material inspection is made.

8.3 Component Tests (U)

(U) During the process of design and fabrication, the Government reserves the right to conduct tests when material and/or methods are being employed which, in the opinion of the Contracting Officer, may not meet the requirements of this Statement of Work, its attachments, or the specifications applicable to each enclosure.

8.4 (U) A preliminary test shall be conducted prior to installation of the interior finishes and full acceptance test upon completion of the enclosure. Testing shall be in accordance with the procedures of NSA Specification No. 65-6 and the acoustic attenuation test portion of NSA Specification 65-5. A test plan shall be submitted for approval and full test report submitted upon completion. Tests shall be performed by Contractor personnel with all required in-calibration test equipment. The Government reserves the right to conduct independent tests to determine the degree of shielding achieved.

8.5 (C) RF leaks will be detected by means of a Contractor-provided TS-31 Monitoring System as manufactured by Quanta Systems. It is understood that the Contractor may have difficulty in obtaining the necessary release in order to acquire the TS-31 system. Should this be the case, the Contractor will immediately notify the Government so that appropriate steps may be taken to assure its release for use on this project. In addition, the Contractor will provide a Shielding Integrity Monitoring System (SIMS) unit, which operates at 462 MHz.

SECTION 9. APPROVAL AND ACCEPTANCE (U)

9.1 Design Approval (U)

(U) The preliminary drawings for each enclosure shall be reviewed and approved by the Contracting Officer or the COTR prior to the manufacturing phase.

9.2 RF and Acoustical Acceptance Tests (U)

(U) The Contractor shall furnish all test equipment and personnel to demonstrate compliance with NSA Specification No. 65-6 and meeting an acoustical attenuation of 45 dB. The number of test frequencies shall be designated by the COTR. The COTR may, at his discretion conduct separate RF and acoustical tests to verify the Contractor's results.

SECTION 10. ADDITIONS AND CORRECTIONS (U)

10.1 (U) Additions and/or corrected drawings, publications, and instructions shall be supplied to the Contracting Officer as soon as the addition and/or correction has been incorporated. Changes made to the enclosure during installation must be reflected in final revised or corrected drawings.

SECTION 11. CAUSE FOR REJECTION (U)

11.1 (U) The work supplied under this contract shall be in all respects, including design, construction, installation, workmanship, performance and quality, in strict accordance with the requirements specified.

11.2 (U) Evidence of non-compliance to specified requirements shall constitute cause for rejection, and it shall be the responsibility of the Contractor to make all necessary corrections at no extra charge to this contract.

SECTION 12. WARRANTY (U)

(U) The RF-shielded enclosure, less moving parts, shall be guaranteed against defective materials and workmanship and to retain the specified shielding characteristics for a period of five years from date of acceptance test.

(U) Moving parts, such as the door, access ports and access panels, shall be guaranteed for a period of one year from date of acceptance test.

SECTION 13. SPECIFIC QUALITY CONTROL (U)

(U) In addition to the general quality control requirements, the Contractor's Quality Control Representative shall perform the following:

a. (U) Verify that all new materials are unused, free from defects and imperfections in workmanship and material.

b. (U) Verify that the workmanship and finish shall be such as to ensure satisfactory operation consistent with the requirement of these specifications. The equipment shall be thoroughly clean and free of excess materials, chips and loose spattered foreign materials. Dissimilar metals shall be protected from galvanic action at contact points.

c. (U) Verify that the mechanics engaged in machining,

welding, supervision, and testing shall have not less than two years of responsible experience in their trades and in the employ of manufacturers of radio frequency shielding building components. Helpers and apprentices shall work under the supervision of responsible mechanics.

d. (U) Verify that the door shall be mated to its frame so as to ensure proper, uniform pressure on all RF seals. Mated assemblies shall be match-marked for installation and all critical measurements recorded, and verified at time of installation.

e. (U) Keep permanent records of receiving inspection of all materials, as well as manufactured assemblies and in-shop tests and inspections. Spot checking of these records shall be performed on site, prior to use in the installation.

SECTION 14. OPERATION AND MAINTENANCE INSTRUCTIONS, PARTS LIST, AND TEST PROCEDURES (U)

a. (U) Operation and maintenance instruction: The instructions shall include complete procedures necessary to operate and maintain the equipment as recommended by the manufacturer. The following sections shall be included, as applicable:

(1) (U) Safety precautions.

(2) (U) Assembly and installation procedures.

(3) (U) Adjustment and alignment.

(4) (U) Routine and preventive maintenance procedures, including a table of recommended frequencies of performing each procedure; e.g., filter cleaning or replacement, lubrication of door mechanisms, etc.

(5) (U) Checkout procedures.

(6) (U) Troubleshooting procedures.

(7) (U) Repair and corrective maintenance replacement procedures.

b. (U) Items of equipment to be described shall include:

(1) (U) Hinges.

(2) (U) Latching hardware.

(3) (U) RF gaskets or seals.

(4) (U) All types of filters.

(5) (U) Panel supporting members.

c. (U) Parts Lists: A parts list shall be furnished which shall include those spares and parts recommended by the manufacturer to assure efficient operation for one year's operation following expiration of the warranty period. This list shall cover components, replacements, supplies, and expendable items as may be required.

d. (U) Test Procedures: Detailed procedures shall be prepared and submitted, covering all tests specified herein, and shall include blank forms for recording and validating the test data.

SECTION 15. GOVERNMENT FURNISHED MATERIAL AND INFORMATION (U)

(U) The Government shall prepare the parent room(s) to accept the RF-shielded enclosure as outlined in attachment E. Specific variations will be addressed on a site-by-site basis.

THIS PAGE INTENTIALLY LEFT BLANK

ATTACHMENT A

GENERAL SPECIFICATIONS FOR RF-SHIELDED ENCLOSURE (U)

SECTION 1. GENERAL (U)

(U) This covers the general requirements applicable to the design and fabrication of an RF-shielded enclosure.

SECTION 2. ENCLOSURE DELIVERY SCHEDULE (U)

(U) The enclosure shall be delivered according to the schedule provided by the Contracing Officer.

SECTION 3. ENCLOSURE MAXIMUM OVERALL OUTSIDE DIMENSIONS (U)

a. (U) Length:
b. (U) Width:
c. (U) Height:

ENTER SITE-UNIQUE INFORMATION HERE

(U) Length shall be within 1 inch of the above value, width shall be within 1 inch of the above value, and height shall be within 1 inch of the above dimension.

SECTION 4. PARENT ROOM DIMENSIONS (See Attachment E) (U)

a. (U) Length:
b. (U) Width:
c. (U) Height:

ENTER SITE-UNIQUE INFORMATION HERE

(U) The parent room dimensions will not be smaller than above values.

SECTION 5. PERSONNEL ACCESS DOOR (U)

(U) The personnel access doors will be as specified in Section 6.3.10 of the Statement of Work.

SECTION 6. ELECTRICAL (U)

a. (U) Three phase electrical service shall enter the enclosure. The main feeders shall be terminated in power distribution panels located as shown in attachment I.

b. (U) The approximate location of the power line filters, power distribution panels and ground stud are shown in attachment I. The Contractor shall determine the quantity of materials (i.e., length of wire and conduit, number of conduit fittings). The Contractor shall include all material necessary to furnish a complete and functional electrical distribution and lighting system. The holes, in the RF wall panel, for the power line filter penetrations and ground stud, shall be cut during field installation.

c. (U) The enclosure light shall be designed for operating on 120V A.C., single-phase, 2-wire (plus equipment ground).

d. (U) All conduit must be surface-mounted ferrous metal conduit, or approved channeling with associated ferrous fittings; EMT (thin wall) is preferred. Fittings must be compression or threaded type. Junction boxes and pull boxes, if required, must be of ferrous metal construction and all knockout openings sealed. All such boxes will be mounted on the enclosure identified in attachment I.

SECTION 7. AIR CONDITIONING PENETRATION (U)

a. (U) Insulated Brass Waveguide Penetrations. The Contractor shall provide insulated brass waveguide penetrations for the air conditioning chilled water supply and return lines. The dimensions, type of material and quantity are to be specified by the Contractor based on type of air conditioning package supplied with enclosure.

b. (U) Noninsulated Brass Waveguide Penetrations. The Contractor shall provide noninsulated brass waveguide penetrations for the air conditioning condensate drain lines. The dimension, type of material and quantity are to be specified by the Contractor.

(U) The holes, in the RF wall panels, for the insulated and noninsulated penetrations shall be cut during field installation.

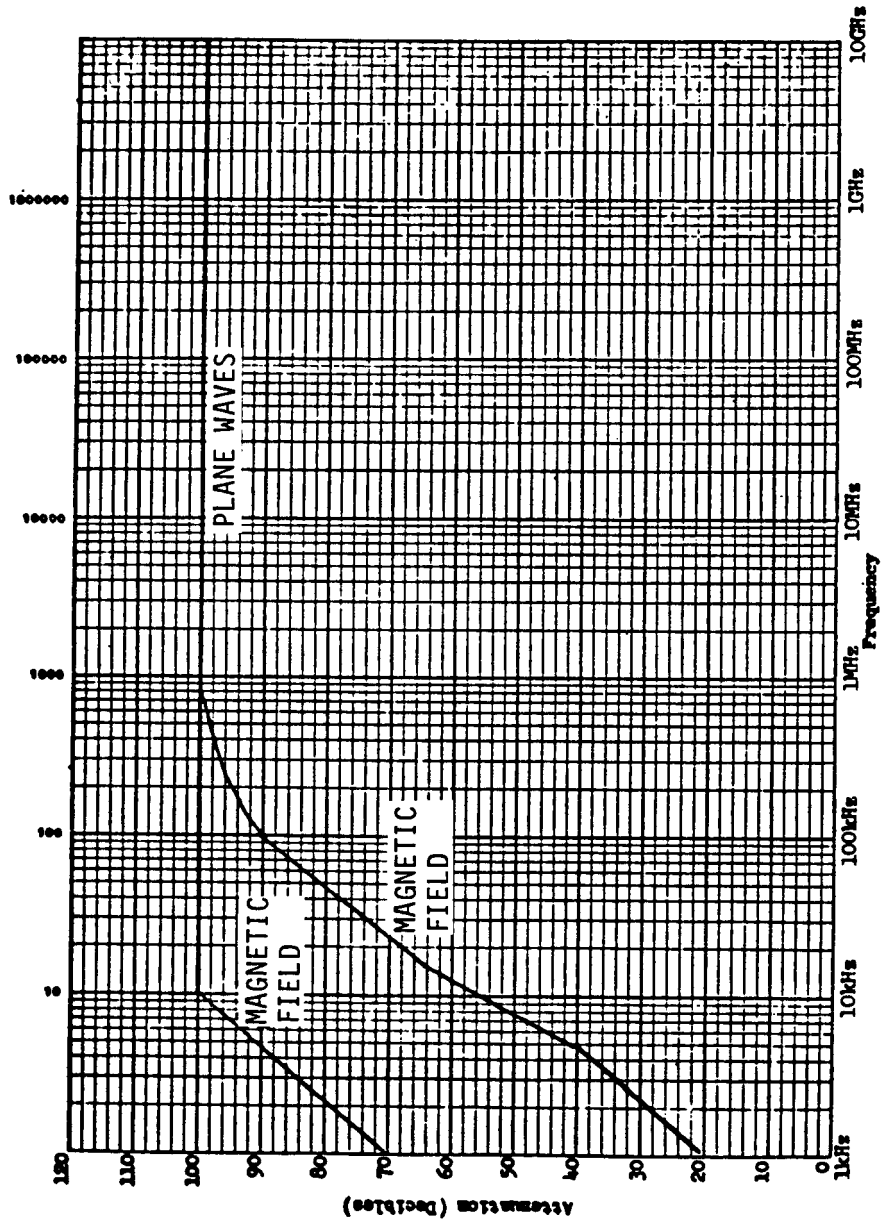
c. (U) Fresh Air Ventilation. Twelve-inch by 12-inch honeycomb air vents shall be provided for fresh air ventilation. The quantity and location of the honeycomb air vents are to be determined by the Contractor based on size and configuration of enclosure. Exhaust fans shall be provided on the honeycomb air vents. The exhaust fans shall be rated to provide one (1) air change in ten (10) minutes. Each honeycomb air vent shall have a flush-fitting type

louvered grill on the interior finished wall. Each intake honeycomb shall have a cleanable, reusable dust filter installed on the outside of the enclosure. Both the intake and exhaust honeycomb air vents shall be acoustically treated, on the exterior of the enclosure only, to meet (or exceed) the acoustic attenuation requirement of attachment C.

THIS PAGE INTENTIONALLY LEFT BLANK

ATTACHMENT B

REQUIRED ELECTROMAGNETIC ATTENUATION (U)

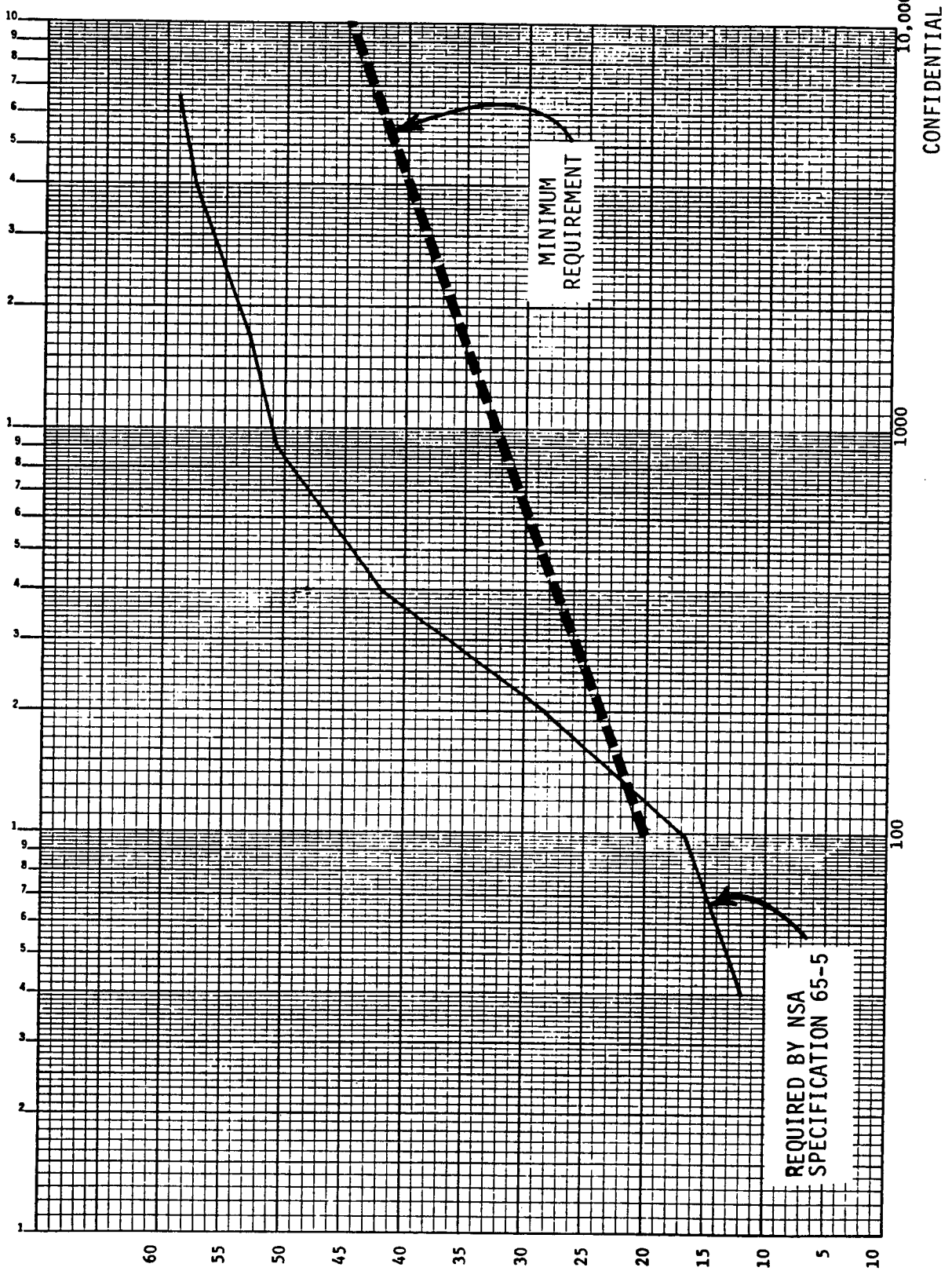


UNCLASSIFIED

THIS PAGE INTENTIONALLY LEFT BLANK

ATTACHMENT C

REQUIRED ACOUSTIC ATTENUATION (U)



THIS PAGE INTENTIONALLY LEFT BLANK

ATTACHMENT D

ENCLOSURE DIMENSIONS (U)

SECTION 1. GENERAL (U)

(C) A platform shall be provided for installation under the enclosure which shall be capable of supporting the enclosure and its contents without buckling or sagging. Platform design shall allow unobstructed surveillance of the area between the underside of the platform and floor of the parent room at all times. There shall be 18 inches of clearance between the floor of the parent room and the underside of the platform. Supporting pillars of the platform shall be transparent. Acoustical isolation shall be provided in the design of the platform to prevent transmission of sound from the enclosure to the floor of the parent room.

(U) The inside vertical dimension of the RF-shielded enclosure will be no less than nine feet, with approximately one foot utilized for a raised floor and approximately six inches utilized for a hung ceiling. Final interior dimensions will be provided by the Project CHOSUN implementation contractor.

SECTION 2. SPECIFIC (U)

(U) The inside dimensions of the proposed enclosure are as shown on the attached drawing and are approximately:

a. (U) Length _____ feet

b. (U) Width _____ feet

c. (U) Height _____ 10 feet*

TYPICAL. ACTUAL DIMENSIONS MUST REFLECT UNIQUE ON-SITE REQUIREMENTS

*(U) Ceiling height is restricted by the presence of structural beams at a height from the floor of 10 feet 5 inches; therefore, the enclosure cannot exceed 10 feet and the lucite support blocks cannot exceed 4 inches.

THIS PAGE INTENTIONALLY LEFT BLANK

ATTACHMENT E

PARENT ROOM (U)

SECTION 1. GENERAL (U)

(U) Unless otherwise specified, the Government will prepare the parent room to accept the RF-shielded enclosure. The Government will furnish to the Contractor architectural drawings depicting: the size and location of AC power service entrances; air handler ducts; existing door openings; signal line, Red ground, and Protected Distribution System (PDS) routing and entrances; and protrusions into the parent room space caused by such items as: pipes, conduit, columns, vertical service chassis, ceiling beams and supports, and the like.

a. (U) The Government's design goal is to provide the Contractor a parent room with a vertical unencumbered dimension of twelve feet, slab-to-slab, within which to assemble an RF-shielded enclosure with a vertical dimension of approximately nine feet.

b. (U) The parent room must provide approximately 18-24 inches of clear space between the outside wall of the RF-shielded enclosure and the inside wall of the parent room.

c. (C) The parent room flooring will be a white linoleum and all adjacent walls and the ceiling area will be painted three coats of white enamel in preparation for the installation of the enclosure.

d. (U) The entire parent room area will be air conditioned by the existing building system. This area is also to be heated and equipped with a building sprinkler system.

SECTION 2. PARENT ROOM DIMENSION (U)

(U) The maximum dimensions of the parent room are as shown on the attached drawing, are to be confirmed by the Contractor by field measurements, and are approximately:

a. (U) Length _____

b. (U) Width _____

c. (U) Height _____

ENTER SITE UNIQUE INFORMATION HERE

SECTION 3. SPECIFIC (U)

ENTER SITE-UNIQUE INFORMATION HERE

ATTACHMENT F

INTERIOR FINISH (U)

	Soundsoak 85
Substrate	Low-density Silok™ mineral fiberboard
Fabric Covering	Embossed needlepunch modacrylic reinforced with woven glass-fiber scrim
Height	9'
Width	24"
Thickness (normal)	1"
Sound Absorption Absorption Coefficients	(125 Hz) .13 / (250 Hz) .41 / (500 Hz) .88 / (1000 Hz) 1.06 / (2000 Hz) .99 / (4000 Hz) .98
Three-Frequency Average (speech privacy range absorption)	.98
Four-Frequency Average	NRC .85
NRC Specification Range	.80-.90
Speech Privacy Noise Isolation Class (NIC) (tested in accordance with PBS C.2 procedure III S)	20
Fire Hazard Classification (ASTM E84 Tunnel Test)	
Flame Spread	25 or less
Fuel Contributed	20
Smoke Density	65
Resistance R	4.00
Installation	Concealed aluminum splines attach to drywall, plaster, brick, block, metal studs, and metal partitions.
Colors	Soft blues or soft greens to enhance video pickup.
Maintenance	Fabric is colorfast to wet and dry-cleaning procedures and most spot-cleaning solvents. Surface Dust: Removed by vacuuming or light brushing. Spots: Dry-cleaning fluid or carpet shampoo. Typical Stains: Coffee, soft drinks, ink crayon, carbon, chewing gum can be completely removed from Soundsoak fabric.

UNCLASSIFIED

THIS PAGE INTENTIONALLY LEFT BLANK

ATTACHMENT G

SERVICE PENETRATIONS (U)

SECTION 1. GENERAL (U)

(U) The quantity, type, and location of all service penetrations shall be determined by the contractor in consonance with the Government's representative. All such penetrations shall conform to the RF-shielding requirements of all enclosures.

SECTION 2. SPECIFIC (U)

ENTER SITE-UNIQUE INFORMATION HERE

THIS PAGE INTENTIONALLY LEFT BLANK

ATTACHMENT H

POWER LINE FILTER SPECIFICATION (U)

SECTION 1. SCOPE (U)

1.1 (U) This specification covers the detailed requirements for RF interference power line filters, hereinafter referred to as "filters," to be used on the RF-shielded enclosures.

SECTION 2. GENERAL INFORMATION (U)

2.1 (U) The filters shall be designed and manufactured in accordance with the latest issue of military specification MIL-F-15733, and shall be capable of meeting full conformance with test procedures as specified in MIL-STD-220A (full load).

SECTION 3. GENERAL REQUIREMENTS (U)

3.1 (U) The filters shall provide a minimum of 100 dB attenuation to all types of signals betweem 14 kHz and 10 GHz at full load.

3.2 (U) The filters shall be designed such that the inductance coils do not saturate under rated load and that the voltage drop across each filter at rated load does not exceed 2.0 volts RMS.

3.3 (U) The filters shall be designed and manufactured for continuous operation at rated load with a temperature rise not to exceed 25 degrees centigrade above ambient.

3.4 (U) The filters shall comply with MIL-F-15733 overload safety requirement for 140 percent rated current for 14 minutes as well as being capable of withstanding short-term current surges in excess of five (5) times rating without damage.

3.5 (U) The filters shall be rated for 250V A.C./600V D.C., 50 or 60 Hz.

3.6 (U) All required filters shall be externally surface mounted at a location designated by the COTR.

SECTION 4. POWER SYSTEMS (U)

4.1 (U) The filters shall be capable of operation on the following power systems:

4.1.1 (U) 120/208V A.C., three-phase, four-wire, 50 or 60 Hz.

SECTION 5. MECHANICAL (U)

5.1 (U) The filter impregnant shall be nonflammable as classified by Underwriters Laboratories, Inc.

5.2 (U) The filter housing shall be fabricated from corrosion resistant finish or nonrusting stainless steel and all seams are to be continuously welded.

5.3 (U) Soft solder shall not be used in the construction of the hermetically sealed portion of the filter case.

5.4 (U) Each filter shall be provided with hermetically sealed alumina electrical terminals and these terminals shall be welded or brazed to the filter case. Soft solder shall not be used to provide a seal for the terminals.

5.5 (U) Both the input and output terminals will be contained within the filter housing.

5.6 Filter Input (U)

5.6.1 (U) The filter housing shall have an access opening to the input terminal large enough to accommodate field installation of the feeder wire. A removable cover shall be installed on the access opening.

5.6.2 (U) A UL-approved solderless electrical lug shall be installed on the input terminal to provide a means for connecting the feeder wire in the field. The lug shall be sized to accept a wire rated at the ampacity of the filter.

5.6.3 (U) Each filter shall have a discharge resistor affixed to its input. The value of the resistor shall be such that the residual energy can be discharged to 90 percent of its maximum value within three seconds after the power is removed from the filter.

5.7 Filter Output (U)

5.7.1 (U) If an access opening is provided to the output terminal within the shielded compartment of the filter housing, it shall have a cover with a gasket between the cover and the cover mating surface to maintain the RF interference integrity of the filter.

5.7.2 (U) A stranded, copper, thermoplastic, insulated-type THW, 600 VAC-rated wire conductor, no less than 48 inches long, shall be installed on the output terminal of the filter. The size of the wire shall be as follows:

a. (U) 50 AMP Filters -- AWG #6

b. (U) 100 AMP Filters -- AWG #2

c. (U) 150 AMP Filters -- AWG #1/10

d. (U) 200 AMP Filters -- AWG #3/0

5.7.3 (U) A threaded pipe waveguide penetration shall be installed on the output side of the filter. Installation hardware (i.e., nuts, washers, gasketing) shall be provided for installing the filters on the shielded enclosure in the field. The diameter of the waveguide through which the wire from the output terminal (paragraph 5.7.2 above) shall be governed by the latest edition of the National Electrical Code. The physical characteristics of the waveguide, the installation hardware, and method of installation shall be such to maintain the RF interference integrity of both the filter and the RF-shielded enclosure.

THIS PAGE INTENTIONALLY LEFT BLANK

ATTACHMENT I

ELECTRICAL DISTRIBUTION (U)

SECTION 1. GENERAL (U)

a. (U) All electrical service within the enclosure shall conform to the current standards outlined in the latest edition of the National Electrical Code Handbook, and shall be in accordance with NACSIM 5203, NACSEM 5204, and NSA Specification No. 65-6. The electrical service within this enclosure shall be provided by a Red distribution system as defined in NACSEM 5203. Electrical service shall be 120/208 volts AC, 60 Hz three-phase "Y." All phases plus the neutral line shall be filtered in accordance with NACSEM 5204 and NSA Specification No. 65-6. The filters shall be installed on the outside of the enclosure. The Red electrical service shall be adequate to provide a three-phase ampere electrical distribution panel, complete with 20 amp circuit breakers. This panel shall be located within the enclosure and appropriately covered to match the decor of the interior of the enclosure.

b. (U) Additional filters shall be furnished as required for the cipher lock/interlock door system and fire detector (ionization). Sufficient duplex outlets shall be provided and installed by the Contractor in accordance with the National Electrical Code Handbook. Physical separation of the electrical distribution service to individual outlets may also be required by the Government's representative. A circuit breaker panel shall be provided and installed adjacent to the filters outside the enclosure by the Contractor. A sufficient quantity of circuit breakers shall be provided to allow a separate circuit breaker for each duplex outlet.

c. (U) The Contractor shall provide a manual trip switch inside the enclosure and in close proximity to the doorway which is capable of interrupting all electrical service within the enclosure. This trip switch will be adequately marked to indicate that it is an emergency shut off switch.

SECTION 2. SPECIFIC (U)

ENTER SITE-UNIQUE INFORMATION HERE

THIS PAGE INTENTIONALLY LEFT BLANK

ATTACHMENT J

AIR CONDITIONING (U)

SECTION 1. GENERAL (U)

(U) Air conditioning facilities for the enclosure(s) shall be provided as specified in the contract. Internal ductwork and waveguides shall be supplied by the enclosure contractor in all cases, and he shall be responsible for ensuring that the air-conditioning installation does not degrade the attenuation of the enclosure.

a. (C) Ductwork. All ductwork shall be designed to provide the acoustic attenuation in compliance with the requirements of attachment C.

b. (U) Waveguides. All air ducts passing through the panels of the enclosure shall be attached to high frequency electromagnetic waveguide cutoff type vents inserted in the enclosure panels to provide RF attenuation in compliance with the requirements of attachment B.

SECTION 2. SPECIFIC (U)

a. (U) The contractor shall provide an air conditioning package capable of easily cooling the enclosure based on the equipment installed within and the average presence of from ____ persons within the enclosure.

b. (U)

ENTER SITE-UNIQUE INFORMATION HERE

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX I

APPROVED TAPE DEGAUSSERS (U)

THIS PAGE INTENTIONALLY LEFT BLANK

(U) This appendix provides a list of approved tape degaussers for CHOSUN. After following the appropriate procedures for degaussing using an approved device, the storage media may be downgraded and released from the controlled environment. This list of approved devices is extracted from DIAM 50-4.

APPROVED TAPE DEGAUSSERS (U)

Company/Model	Adapter for Floppy Disks	Adapter for Cassettes	Adapter for Mag Cards
a. Ampex/SE20			NSA Drawing 98230-ON126996
b. Bell & Howell/ TD-2903-4B	P/N 529872	P/N 531972	NSA Drawing 98230-ON126996
c. Computer Link Corp./ 515	Attachment Supplied	Attachment Supplied	NSA Drawing 98230-ON126996
d. Consolidated Electro-dynamics/TD-2903-4A, TD-2903-4B	P/N 529872	P/N 531072	NSA Drawing 98230-ON126996
e. Data Devices Int./ Cambrian	P/N 529872	P/N 531072	NSA Drawing 98230-ON126996
f. General Kinetics Inc./ K80 (see note 4)	Not required	K80-R	NSA Drawing 98230-ON126996
g. Electro Matics Products/2PTFB15-17, 2PTFB15-18	Not required	Not required	Not required
h. Hewlett Packard/3603A			

Declassified and Approved For Release 2011/11/10 : CIA-RDP96B01172R000400050018-5

Notes:

1. (U) All of the above models except "a." are 50 or 60 Hz line frequency, but the frequency to be used must be specified at the time of procurement.

2. (U) The models under "g." should be certified by NSA/CSS(L14) immediately after installation. These larger conveyorized degaussers, while more costly, are more suitable for large DPIs processing tapes in large quantites because their processing speed permits them to handle up to 20 tapes per minute as contrasted to the less expensive devices, which normally process one tape per minute.

3. (U) Always take precautions to insure that tape degaussers are operating properly.

4. (U) When using GKI Model K80 degausser for tapes wider than 1/2 inch, turn the tape over and degauss it again.

5. (U) Item "c." is the only model that includes an adapter.

6. (U) The degaussers noted above are not acceptable for the erasure of high energy tape, or tape with a coercivity greater than 325 oersteds.

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX J

SPECIFICATIONS FOR MAGNETIC TAPE ERASE EQUIPMENT (U)

THIS PAGE INTENTIONALLY LEFT BLANK

(U) This specification, extracted from DIAM 50-4, covers any equipment to be used for automatic bulk degaussing of recorded magnetic tape. It describes, in general, the desired configuration and sets forth desired electrical and magnetic performance.

J.1 Requirements (U)

J.1.1 (U) General.

a. (U) Reel Size. The equipment shall be designed to degauss magnetic tape in widths from 1 to 2 inches, wound on reels from 3 to 15 inches in diameter, with provision for conversion to either 5/16-inch hubs or computer reel hub dimensions. It will be permissible to turn over 2-inch reels for degaussing.

b. (U) Installation. The equipment shall be designed such that either rackmounting or bench top operation can be accommodated with minimum modification.

c. (U) Operation. Operation shall be automatic once the reel is loaded and the degaussing cycle is initiated, except for 2-inch-wide tape which may be cycled twice. The degaussing operation shall not require more than two minutes per reel.

d. (U) Degaussing Safeguard. A method of monitoring the relative current in the degaussing coils shall be provided.

e. (U) Safeguard Tape Unwinding. For vertically mounted degaussers, a method of reversing the direction of reel rotation while cycling shall be provided. This reversal of reel direction must not interrupt the degaussing cycle. This safeguard prevents the unwinding of tape while cycling.

J.1.2 (U) Electrical Power. The equipment must meet all requirements over the following parameter ranges:

a. (U) Input Voltage Range - 95 to 135 VAC, single phase, three-wire system.

b. (U) Line Frequency Range - 48 to 62 cycles per second.

c. (U) Power - The current drain shall be less than 20 amperes for any of the foregoing conditions of line frequency and voltage.

J.1.3 (U) Mechanical.

a. (U) Cabinet. The equipment shall be designed for mounting in a standard 19-inch rack and shall have minimum height and weight according to the design requirements.

b. (U) Finish. Surfaces shall be adequately protected against corrosion within the environments detailed under section J.1.4 below.

J.1.4 (U) Environmental Performance. The equipment shall perform to specification when operated in the environments listed in the following paragraphs:

a. (U) Altitude. Non-operating: sea level to 50,000 feet
Operating: sea level to 10,000 feet

b. (U) Relative Humidity. Operating and non-operating: 5 to 100 percent, no condensation. However, the equipment shall survive condensation after being dried out.

c. (U) Temperature. Non-operating: -40^0 to 71^0 C
Operating: 0^0 + 55^0 C

d. (U) Vibration and Shock. Non-operating. The equipment shall survive specified test methods which are intended to simulate shock and vibration levels expected in commercial shipping and handling.

J.1.5 (U) Performance.

a. (U) Degaussing Level. The residual signal level after degaussing shall be a minimum of 90 db below saturated signal level for tape widths of 1 inch or less.

b. (U) Duty Cycle. Design shall be such that continuous operation (i.e., a duty cycle of 100%) may be used. Under conditions of continuous operation, the temperature rise at the reel face of the equipment shall not exceed 35^0F above ambient.

J.2 Test Procedures (U)

J.2.1 (U) Equipment.

a. (U) Recorder/reproducer with full track 1/4" heads.

b. (U) Audio oscillator.

c. (U) Wave analyser with 20 Hz bandwidth.

d. (U) Oscilloscope.

J.2.2 (U) Procedure.

a. (U) Record. Record tapes with a 400 Hz signal at 7 ips with the record level set for saturation. Measure the playback signal level using the wave analyzer on the 20 Hz bandwidth position and the recorder playback gain set at maximum. This is the reproduce reference level.

(U) NOTE: The saturation point shall be defined by the tape transfer curve as the output level for which input levels L and 2L produce the same output.

b. (U) Degaussing. Degauss the tapes.

(U) NOTE: To evaluate the ability to degauss wider tape widths, two, three, and four 1/4-inch reels can be taped together for the degaussing procedure. To simulate the larger diameter reels a special 15-inch X 1/4-inch reel would have to be used. This can be constructed by interchanging a standard 1/4-inch hub and 15-inch flanges.

c. (U) Playback. Play back the degaussed tapes with the play back gain set at maximum. Tune the wave analyzer (20 Hz bandwidth) to measure any residual signal level.

(U) NOTE: Clean and degauss tape recorder threading path before each pass.

APPENDIX K

APPROVED DISK PACK DEGAUSSERS (U)

THIS PAGE INTENTIONALLY LEFT BLANK

(U) This appendix provides a list of approved disk pack degaussers for CHOSUN. After following the appropriate procedures for degaussing using an approved device, the storage media may be downgraded and released from the controlled environment. This list of approved devices is extracted from DIAM 50-4.

APPROVED DISK PACK DEGAUSSERS (U)

a.	Brown Baverl-Recoma, Inc./ON261059	- Disks and Drums -
b.	Precision Methods, Inc./2000	- Disks and Drums -
c.	Precision Methods, Inc./1500	- Disks only -
d.	Jobmaster Corp./42-P-MEM	- Disks only -
e.	Jobmaster Corp./4744H	- Drums only -

Notes:

1. (U) All of the above models are 50 or 60 Hz line frequency, but the frequency to be used must be specified at the time of procurement.

2. (U) Items a and b are also suitable for erasure of magnetic drums. Although the permanent magnetic devices have a very strong magnetic field, they are not acceptable for the erasure of other types of magnetic storage media and should be used only for disks and drums.

3. (U) To erase disk packs, cover the magnetic assembly with a lintless wiping tissue with a thickness no greater than .36mm (.014 inches) to prevent damage to the recording surface(s). Insert the degaussing wand into the disk so the active magnetic portion completely covers the recording surface of the disk from the hub to the perimeter. Wipe each active disk surface (top and bottom) at least three times with the magnetic eraser.

4. (U) To erase drums, cover the magnetic assembly with a lintless wiping tissue with a thickness no greater than .36mm (.014 inches) to prevent damage to the recording surface(s). While **slowly** rotating the drum, wipe the entire surface at least three times with the magnet. Be sure that all recording areas of the drum are exposed to the active area of the magnetic area.

Declassified and Approved For Release 2011/11/10 : CIA-RDP96B01172R000400050018-5

UNCLASSIFIED

APPENDIX L

APPROVED PAPER DESTRUCTION DEVICES (U)

UNCLASSIFIED

THIS PAGE INTENTIONALLY LEFT BLANK

(U) This appendix contains a list of types of equipment which have been tested and approved by the National Security Agency and which, when equipped as specified, meet the routine destruction standards for paper COMSEC materials.

(U) Approval of a specific equipment has been based only on examination of residue and a physical security evaluation of the equipment. Such factors as reliability, rate of wear, and frequency of key part replacement have not been evaluated, and NSA does not endorse manufacturers' claims concerning these aspects. Hourly volume rates stated are estimates based on average rates for destruction of paper materials and may vary depending on variety, volume, and loading.

(U) Other equipment will be added to this list as it is evaluated and approved. Queries or information concerning equipment not shown on the list may be addressed to the Director, National Security Agency, ATTN: S133, Fort George G. Meade, MD 20755.

(U) Many, though not all, of the devices listed are available from the GSA Federal Supply Schedule.

NSA-APPROVED PAPER DESTRUCTION DEVICES (U)

EQUIPMENT DESIGNATION	MANUFACTURER OR DISTRIBUTOR	CAPACITY LBS PER HOUR	REMARKS
Air Fed Model 3 Incinerator	Buffalo Metal Fabricating Corp. 50 Wecker Street Buffalo, NY 14215	6	
Waring 7-Speed Blender	Waring Products Division Dynamics Corporation of America New Hartford, CT 06057	15	Not approved for high wet strength paper.
Destroyit Cross Cut Shredder	The Michael Lith Sales Corp. 145 West 45th Street New York, NY 10036	25	
Shredmaster Cross Cut 200 Shredder	Shredmaster Corp. 1101 Skokie Boulevard Northbrook, IL 60062	25	
Security Engineered Model 700	Security Engineered Machine Co. 5 Walkup Drive Westboro, MA 01581	50	Office Model. Low noise level.
Security Engineered Dry Disintegrator Model 1	Security Engineered Machine Co. 5 Walkup Drive Westboro, MA 01581	50	3/32" filter screen required. Sound enclosure available.
Jay-Bee Model MB2 and MB3 Office Disintegrator	Jay-Bee Manufacturing Co., Inc. P.O. Box 986 Tyler, TX 75701	50-75 75-100	3/16" filter screen required. Moderate noise level.

EQUIPMENT DESIGNATION	MANUFACTURER OR DISTRIBUTOR	CAPACITY LBS PER HOUR	REMARKS
Intimus #007 Shredder (Cross Cut)	Whitaker Bros. Business Machines Inc. 5913 Georgia Avenue, NW Washington, DC 20011	75	Also marketed as the Cummins Model 48 Shredder.
Jay-Bee Model AB Disintegrator	Jay-Bee Manufacturing Co., Inc. P.O. Box 986 Tyler, TX 75701	75-150	Discontinued. 3/16" filter screen required. High noise level and some dust.
Air Fed Model 2 Incinerator	Buffalo Metal Fabricating Corp. 50 Wecker Street Buffalo, NY 14215	85-120	
Security Engineered Dry Disintegrator Model 2	Security Engineered Machinery Co. 5 Walkup Drive Westboro, MA 01581	100	3/32" filter screen required. Sound enclosure available.
Jay-Bee Model 3CB Disintegrator	Jay-Bee Manufacturing Co., Inc. P.O. Box 986 Tyler, TX 75701	200	3/16" filter screen required. High noise level.
Security Engineered Dry Disintegrator Model 3	Security Engineered Machinery Co. 5 Walkup Drive Westboro, MA 01581	200	Discontinued. 3/32" filter screen req. High noise level.
SOMAT Model 30 IS Pulper	SOMAT Corporation Box 831 Coatsville, PA 19320	200	Discontinued. Not approved for high wet strength paper. 5/16" ring hole strainer required.

EQUIPMENT DESIGNATION	MANUFACTURER OR DISTRIBUTOR	CAPACITY LBS PER HOUR	REMARKS
Air Fed Model 1 Incinerator	Buffalo Metal Fabricating Corp. 50 Wecker Street Buffalo, NY 14215	200-450	
Jay-Bee Model 2 ISW Disintegrator	Jay-Bee Manufacturing Co., Inc. P.O. Box 986 Tyler, TX 85801	300	3/16" filter screen required. High noise and dust levels. Destroys printed circuit boards when equipped with appropriate filter screen.
Security Engineered Disintegrator Model 1012	Security Engineered Machine Co. 5 Walkup Drive Westboro, MA 01581	400	3/32" filter screen required. Sound enclosure available.
Jay-Bee Model 3 ISW Disintegrator	Jay-Bee Manufacturing Co., Inc. P.O. Box 986 Tyler, TX 85801	750	3/32" filter screen required. High noise and dust levels. Destroys printed circuit boards when equipped with appropriate filter screen.
Security Engineered Disintegrator Model 22	Security Engineered Machinery Co. 5 Walkup Drive Westboro, MA 01581	600	3/32" filter screen required. Sound enclosure available. Destroys printed circuit boards when equipped with appropriate filter screen.

EQUIPMENT DESIGNATION	MANUFACTURER OR DISTRIBUTOR	CAPACITY LBS PER HOUR	REMARKS
DDS Hammermill Model 12	Document Disintegration Systems 2075 Belgrave Avenue Huntington Park, CA 90255	600	Discontinued. 3/16" filter screen required . High noise and dust levels. Destroys printed circuit boards when equipped with appropriate filter screen.
Security Engineered Disintegrator Model 1424	Security Engineered Machinery Co. 5 Walkup Drive Westboro, MA 01581	800	3/32" filter screen required. Sound enclosure available. Destroys printed circuit boards when equipped with appropriate filter screen.
DDS Hammermill Model DDS-18	Document Disintegration Systems L&F Industries 2075 Belgrave Avenue Huntington Park, CA 90255	1000	Equipped with 3/16" filter screen. High noise and dust levels. Destroys printed circuit boards when equipped with appropriate filer screen.
Jay-Bee Model 4 ISW Disintegrator	Jay-Bee Manufacturing Co., Inc. P.O. Box 986 Tyler, TX 75701	1500	3/16" filter screen required. High noise and dust levels. Destroys printed circuit boards when equipped with appropriate filter screen.
DDS Hammermill Model DDS-24	Document Disintegration Systems 2075 Belgrave Avenue Huntington Park, CA 90255	2300	3/16" filter screen required. High noise and dust levels. Destroys printed circuit boards when equipped with appropriate filter screen.

UNCLASSIFIED

Declassified and Approved For Release 2011/11/10 : CIA-RDP96B01172R000400050018-5

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX M

GLOSSARY (U)

AC/DC	Alternating Current/Direct Current
ADP	Automatic Data Processing
C	Confidential
CCSO	Command and Control Systems Organization
CNWDI	Critical Nuclear Weapon Design Information
COMSEC	Communication Security
CTCO	Central Technical Control Operator
CZ	Controlled Zone
DAA	Designated Approving Authority
dB	decibel
DCA	Defense Communications Agency
DCI	Director of Central Intelligence
DCID	Director of Central Intelligence Directive
DES	Data Encryption Standard
DIAM	Defense Intelligence Agency Manual
DPI	Data Processing Installation
EMC	Electromagnetic Compatibility
EMI	Electromagnetic Interference
EMSEC	Emanations Security
FRD	Formerly Restricted Data
GSA	General Services Administration
HISSO	Hub Information System Security Officer
Hz	Hertz
ips	inches per second
IST	Independent Security Test
MIL-STD	Military Standard
NAC	National Agency Check
NACSEM	National COMSEC/EMSEC Information
NACSI	National COMSEC Information
NCO	Network Control Operator
NCSC	National Communications Security Committee
NCWG	Network Certification Working Group
NDA	Non-Disclosure Agreement

NFIB	National Foreign Intelligence Board
NFIC	National Foreign Intelligence Committee
NISSO	Node Information System Security Officer
NSA	National Security Agency
NSA/CSS	National Security Agency/Central Security Service
NSC	National Security Council
NSDD-95	National Security Decision Directive 95
NSO	Network Security Officer
OADR	Originating Agency's Determination Required
OMB	Office of Management and Budget
OPR	Office of Primary Responsibility
OT&E	Operational Test and Evaluation
PDS	Protected Distribution System
PM	Program Manager
PMO	Program Management Office
PPL	Preferred Products List
PR	Periodic Reinvestigation
RD	Restricted Data
RF	Radio Frequency
S	Secret
SCI	Sensitive Compartmented Information
SCO	System Control Operator
SCIF	Sensitive Compartmented Information Facility
SCOCE	Subcommittee on Compromising Emanations
SOP	Standing Operating Procedures
ST&E	Security Test and Evaluation
STC	Sound Transmission Class
TCO	Technical Control Operator
TQSC	TEMPEST Qualification Special Committee
TS	Top Secret
TSA	Temporary Secure Area
U	Unclassified
UCT	User Control Terminal
UPS	Uninterruptible Power Supply
WAWS	Washington Area Wideband System