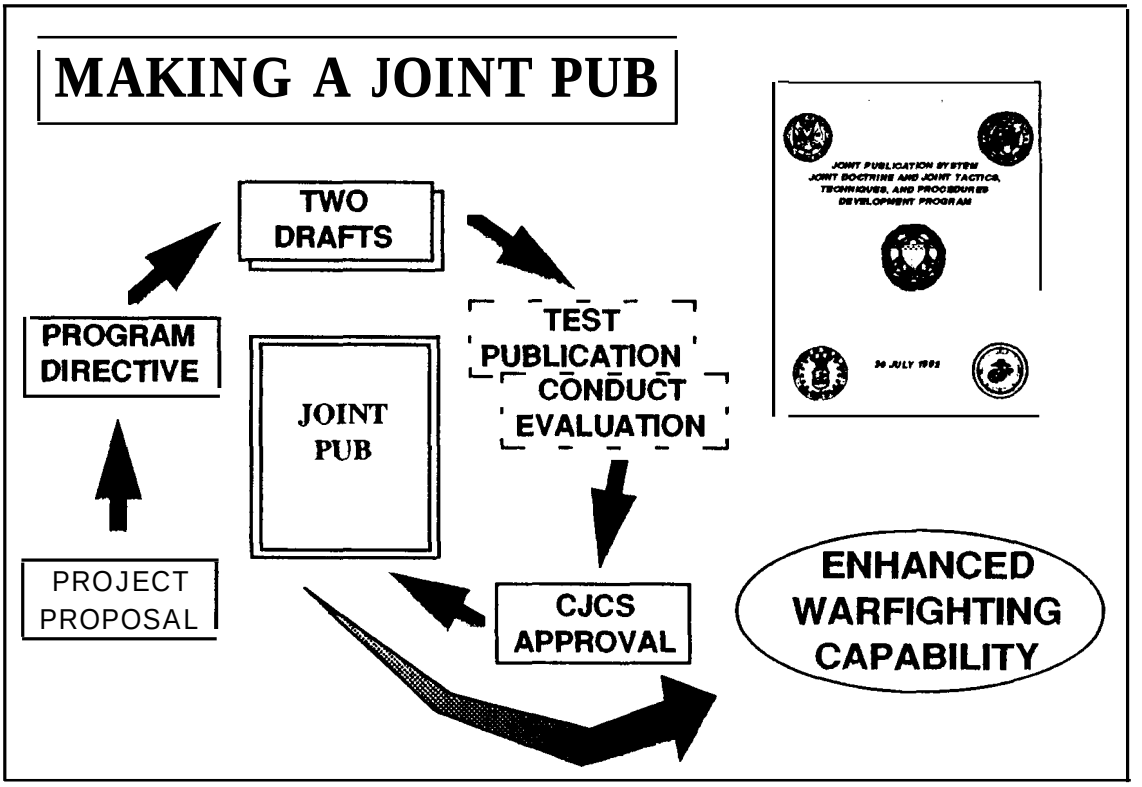
JOINT PUB 6-03.7

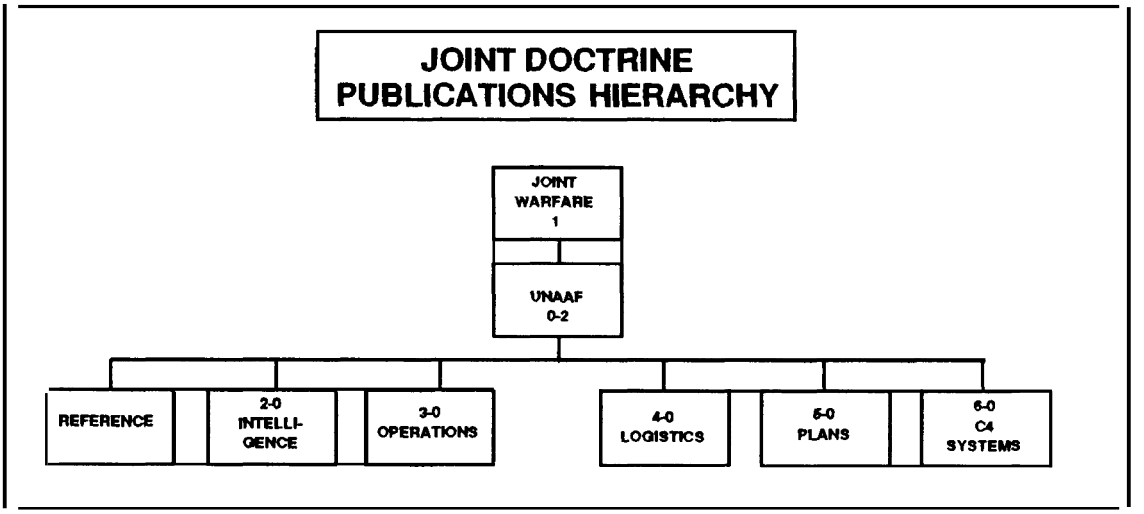
SECURITY POLICY FOR THE WWMCCS INTERCOMPUTER NETWORK

14 JANUARY 1993

A large body of joint doctrine (and its supporting tactics, techniques, and procedures) has been and is being developed by the US Armed Forces through the combined efforts of the Joint Staff, Services, and combatant commands. The following chart displays an overview of the development process for these publications.



All joint doctrine and tactics, techniques, and procedures are organized into a comprehensive hierarchy. Joint Pub 3–04 .1 is located in the operations series of joint publications .



Joint Pub 1–01, "Joint Publication System, " provides a detailed list of all joint publications. Joint pubs are also available on CD–ROM through the Joint Electronic Library (JEL) . For information, contact : Joint Doctrine Division, J-7, 7000 Joint Staff Pentagon Washington, D. C. 20318–7000 .

Reply ZIP Code:
20318-0400

Joint Pub 6-03.7

MEMORANDUM FOR: Distribution List

Subject: Joint Pub 6-03.7, "Security Policy for the WWMCCS Intercomputer Network"

1. This publication has been prepared under the direction of the Chairman of the Joint Chiefs of Staff. It sets forth principles and military guidance to govern the joint activities and performance of the Armed Forces of the United States.

2. Recommendations for changes to this publication should be submitted to the Director for Command, Control, Communications, and Computer Systems (J-6), Joint Staff, Washington, D.C. 20318-6000.

3. The Military Services and other Defense agencies are requested to notify the Director, J-6, Joint Staff, when changes to source documents reflected in this publication are initiated.

4. Additional copies of this publication can be obtained through Service publication centers.

5. This publication supersedes Joint Pub 6-03.7, April 1988.

6. The lead agent and Joint Staff doctrine sponsor for this publication is J-6.

For the Chairman of the Joint Chiefs of Staff:

H. L. SHEFFIELD
Captain, USN
Secretary, Joint Staff

Enclosure

(INTENTIONALLY BLANK)

SECURITY POLICY FOR THE WWMCCS INTERCOMPUTER NETWORK

PREFACE

1. Purpose. This publication provides minimum AIS security requirements necessary to protect WIN resources (equipment, personnel, data, etc.) from denial of use, damage, tampering, espionage, fraud, misappropriation, misuse, unauthorized modification, and unauthorized disclosure.

2. Application. The provisions of this publication will be followed by authorized users of WIN resources. Each terminal or workstation area will have a copy of this publication available for users' reference.

3. Scope. This publication establishes the Director, J-6, Joint Staff, as the highest DAA for WIN security and operations. It identifies the roles and responsibilities of the WIN DAA, Services, Defense agencies, Combatant Commands, the WASO, local DAAs, terminal area certification authorities or DAAs, WASSMs, WASSOs, WATASOs, users, and customers.

4. Basis. This publication implements DOD Directive 5200.28, DOD 5200.1-R, ISOO Directive No.1, OMB Circular No. A-130, and Public Law 100-235.

(INTENTIONALLY BLANK)

TABLE OF CONTENTS

(INTENTIONALLY BLANK)

CHAPTER I

GENERAL PROVISIONS

1. Introduction. The WIN is a centrally managed information processing system of networked mainframe computers, network monitoring facilities, LANs, workstations, terminals, and other peripheral devices. The mainframe computers are interconnected by a wideband, packet-switched TOP SECRET system high security mode communications subsystem of DDN. The WIN processes information classified up to and including TOP SECRET. (Special Access Programs established in accordance with DOD 5200.1-R, information that should be labeled WNINTEL, and foreign government classified information are not permitted.) Because the WIN processes and communicates classified information and is vulnerable to a host of threats ranging from physical and environmental hazards to malicious software, an effective INFOSEC program must be implemented. Accordingly, the WIN DAA publishes the WIN security policy in this document.

2. Purpose. This publication sets forth the minimum security safeguards required for participation in the WIN. These safeguards implement a secure ADP system that performs the operational mission of the WIN while providing for confidentiality, availability, and integrity of data. Because system security requirements sometimes clash with users' operational requirements, the ultimate question becomes whether to accept additional risks with increasing operational capabilities. Decisions on these issues should not be avoided, but should be brought expeditiously to the appropriate DAA for resolution. Policy in this publication will guide the DAA in making these resolutions.

3. Scope

a. Policy Application. This policy applies to all WIN users. The requirements of this publication are considered the minimum essential for WIN connections.

(1) Remotely Connected AISs. For users connected to the WIN remotely through other AISs, the requirements of this publication will apply as specified in the MOA between the WIN site DAA and the DAA of the connected AIS.

(2) Service and Defense Agency Policy. Services, Defense agencies, and commands are encouraged to implement their own additional security requirements. In case of conflict, the more stringent policy will apply. If two WIN sites covered by different Service or Defense agency

security policies are involved, either the more stringent will apply or the two DAAs may sign an MOA whose security policy is at least as stringent as Joint Pub 6-03.7.

(3) CINC Policy. CINC WIN sites will either comply with their supporting Service ADP security regulation (e.g., AR 380-19) or prepare a CINC-approved regulation as stringent as the applicable Service regulation. If the latter, the J-6, Joint Staff, will be placed on the distribution list.

(4) Other Non-WIN WWMCCS ADP AISs. Other non-WIN WWMCCS AISs will be covered by regulations issued by the appropriate DOD component DAA.

b. WIN Policy Boundary. From the security policy standpoint, the WIN boundary extends as described below:

(1) It includes WIN computers (see Chapter III, subparagraph 1b) or LANs requiring connection to the WIN and having as their primary purpose a requirement to run some WIN standard software.

(2) It extends only to the interfaces to other non-WIN AISs such as the WINCS. For those non-WIN AISs connected to the WIN, security policy requirements will be addressed in the MOA between the WIN site DAA to which it is attached and the DAA of the connected AIS.

4. Authority. Authority for publication of this document rests in the DOD publications listed in Appendix A.

5. Life-Cycle Management

a. Security Planning. Security planning is an essential part of a program, system, development project, or procurement action. INFOSEC will be addressed by DAAs, program managers, and security personnel in each phase of the system life cycle: concept development, design, development, and operations phase. Security in the acquisition or development process is based on the following concepts:

(1) INFOSEC is an operational requirement and should be treated with the same thoroughness as other operational performance issues.

(2) To be cost effective, INFOSEC should be addressed as early as possible in the concepts definition phase of acquisition and continually

refined throughout the acquisition and development process.

b. DAA Involvement. Early and continual DAA involvement in the security aspects of acquisition or development will assist the DAA in developing the background understanding necessary for a sound accreditation decision. DAAs should be aware of the effectiveness of proposed safeguards, the attendant risks, and the rationale supporting their approval.

c. Contractual Considerations

(1) Security Requirements. Security requirements depend on the system being developed, security mode(s) (defined in Chapter III) being implemented, classification of information to be protected, and the degree of trust (DOD Trusted Computer System Evaluation Criteria) under which the system will operate. Often, tradeoffs may have to be made between the degree of security provided to protect the information resident in the system and other mission requirements. Cost studies and risk analyses will be performed to determine the most cost-effective method and type of security protection to implement. Requirements will be complete and unambiguous and will include objective criteria or metrics (numerical values) whenever possible to facilitate testing and validation.

(2) RFPs. RFPs contain proposed, contractually binding requirements. When an RFP is prepared, the appropriate program manager will make sure that:

(a) Specific security-oriented requirements, such as intended security attributes (e.g., security-related functional and assurance requirements), are included in the SOW.

(b) The contract is specifically tailored so that results of required studies are explicitly called for in appropriate design reviews. Requirements for cleared facilities, contractors with clearances, and hardware and software configuration control will be explicitly stated. If detailed security requirements are not adequately presented in contractual documents or are changed after contract award, reviews can be used to obtain the necessary security information. More detailed guidance can be obtained in the appropriate DOD publications.

6. Security Technical Assistance. DOD components requiring computer security technical assistance have various organizations available to contact. NSA has suborganizations that specialize in computer and communications security. The Services and Defense agencies have computer security offices that can provide assistance. DISA has responsibility for providing assistance in many areas covered by this publication (see Chapter II, paragraph 5). The Joint Staff WASO will also provide support in obtaining security technical assistance, as required.

7. Requests for Waiver. Portions of this policy requiring formal waiver, as well as the level at which that waiver authority is executed, are provided in Appendix G.

a. Risk Analysis Report. Current site DAA waivers will be documented in the Risk Analysis report.

b. Request Via the Chain of Command. Organizations requiring waivers from the Joint Staff will request them in writing from the J-6, Joint Staff (WIN DAA). Waiver requests to the Joint Staff from RNP/Remote DATANET-8/ Concentrator/LAN Sites and terminal areas must include approval from their respective accrediting multiuser hosts and each organization within their respective chains of command. (RNP/Remote DATANET-8/ Concentrator/LAN Sites and terminal areas will not submit waiver requests directly to the Joint Staff.)

c. Duration. Duration of Joint Staff waivers will generally not exceed 12 months and must stipulate special conditions associated with the waiver.

d. Classification. Requests for waivers will be classified in accordance with Appendix B.

e. Justification. The basis for requesting a waiver to the requirements of this publication will be that operational or mission considerations outweigh the security risk(s) involved.

f. Alternative protection. Alternative protection methods will be provided to safeguard information affected by the waiver. At a minimum, requests for a waiver will contain the following:

(1) Statement of Requirement. Identification of the requirement for which the waiver is requested.

(2) Reference Document. The reference document (chapter, section, paragraph) that cites the requirement.

(3) Effect on Operations. Description of specific operational and technical difficulties that will result if compliance with the security requirement is enforced; e.g., "It will not be possible to submit timesharing jobs" or "It will take 10 minutes longer to log on to the system." Use objective criteria or metrics (numerical values) in lieu of general statements to illustrate effects described in narrative form.

(4) Mission Impact. Mission impact resulting from the difficulties identified in subparagraph I-7f(3) above. Generalizations such as "Mission will be severely hindered" are to be avoided. State specifically:

(a) What will not be accomplished.

(b) What will be delayed.

(c) The net effect of failure or delay in meeting operational objectives.

g. Alternatives. To ensure that a waiver is the only acceptable solution to noncompliance with a requirement of this publication, at least two alternatives will be identified in the waiver package. With the assistance of a WASSO or WASSM, a thorough assessment of these alternatives will be conducted. An analysis of cost, effect on operations, mission impact, and security will convincingly show that a waiver is necessary.

h. Connections to Other Applications. Identify connections to other systems or networks. Identify effects this waiver may have on security safeguards implemented on those systems.

i. Expected Duration of the Waiver. Address actions being taken to correct the waiverable condition and include the date the waiver is expected to expire.

j. Written Review by the WASSO or WASSM. Waiver requests will be reviewed and signed by the WASSO or WASSM of the submitting organization.

8. Security Incident Reports

a. General. Security incidents will be investigated in accordance with Service or Defense agency directives to determine their cause and the corrective action to be taken. Incidents caused by a failure of WIN standard and nonstandard hardware or software will be reported in accordance with Joint Pub 6-03.11. Incidents affecting

two or more WIN multiuser host sites will be reported to the WASO. Incidents will be fully documented so that areas requiring special corrective action can be identified. If compromise of classified material is suspected, a report of facts surrounding the incident will be immediately forwarded to a responsible official with a copy to the WASO. A preliminary inquiry will then be conducted in accordance with DOD 5200.1-R.

b. Security Incident Categories. Initially, network incidents will be divided into one of the following three categories:

(1) Minor event, where an explanation is obvious or satisfactory and normally handled by other than security action.

(2) Nonroutine events requiring WASSO action.

(3) Compromise event, where intent or effect is suspicious or where compromise or possible compromise of classified information has taken place.

c. Actions. The WASSO will immediately inform the affected OPRs of significant security incidents (subparagraphs 8b(2) and (3) above) that involve their files.

9. WIN Security Technical Procedures

a. Purpose. WIN STPs define specific security guidance and procedures that implement security policies specified in this and other DOD publications. They will not be used to promulgate security policies.

b. Authority. The WIN DAA is authorized to publish WIN STPs.

c. Coordination. STPs may be initiated by the WASO or WASSOs. Coordination between WASSOs before publication will be accomplished by the WASO. Technical support in drafting STPs will be provided by the DISA.

10. Amendments. Joint Pub 6-03.7 will be amended as required. Unless otherwise specified, amendments will be effective upon publication. Recommendations for future amendments are encouraged and should be forwarded to the Joint Staff WASO for consideration.

11. Reproduction and Extracts. Local reproduction of this publication and the STPs is authorized for government use

(INTENTIONALLY BLANK)

CHAPTER II

RESPONSIBILITIES

1. Chairman of the Joint Chiefs of Staff. The Chairman of the Joint Chiefs of Staff will:

   a. Develop and disseminate overall WIN security policy.

   b. Establish WIN security requirements for WWMCCS ADP system developers such as DISA, USTRANSCOM, and the WWMCCS ADP PMO.

2. Director for C4 Systems, J-6, Joint Staff. The Director for C4 Systems, J-6, Joint Staff will:

   a. Serve as the WIN DAA.

   b. Approve WIN interconnections with other non-WWMCCS AISs via MOAs to ensure that these connections do not degrade security or operational capability.

   c. Accredit major modifications to the WIN.

   d. Accredit WIN multiuser host sites for network connectivity.

   e. Appoint a WASO.

   f. Approve STPs as described in Chapter I.

3. Chiefs of the Services, CINCs, and Directors of Defense Agencies. The Chiefs of the Services, CINCs, and Directors of Defense agencies will:

   a. Ensure that an official is designated as a WIN local site DAA to fulfill DOD Directive 5200.28 and Joint Pub 6-03.7 responsibilities for WIN elements under their jurisdiction.

   b. Ensure that provisions of Joint Pub 6-03.7 are implemented.

   c. Ensure that WIN multiuser host and RNP sites are adequately staffed with a WASSO and ADP security specialists to implement this publication.

   d. Ensure that proposed changes to WIN site hardware and software configurations are approved in accordance with Joint Pub 6-03.11.

4. Commander, Air Training Command. As the WIN's Single Service Training Manager, the US Air Force will provide for the security-related training of individual users.

5. Director, Defense Information Systems Agency. The DISA will:

a. Provide centralized security technical support for the development, maintenance, test, evaluation, and use of all components of the WIN.

b. Review specifications for software and hardware security features.

c. Perform ST&Es for standard software releases.

d. Evaluate SDNs for security and provide results to the J-6, Joint Staff.

e. Evaluate WIN security incident reports that deal with technical and system software issues and provide recommendations to the WASO.

f. Perform security tests on standard WIN hardware and software as required by J-6, Joint Staff. (TEMPEST testing is not included.)

g. Develop, install, analyze, test, and evaluate prototype ADP security protection systems for the WIN in conjunction with the appropriate Services, unified and specified commands, and Defense agencies.

h. Provide software capable of declassifying and regrading standard WIN hardware and removable media. Certify to the J-6, Joint Staff, that this software performs as specified before field use and serve as its configuration manager. A current list of this software will be provided to all WASSOs.

i. Support the WASO by maintaining technical cognizance of all aspects of computer network security, including hardware, software, COMSEC, and EMSEC.

j. Evaluate specialized ST&E tools for use on the WIN.

k. Provide written technical ADP security evaluations of WIN multiuser host certification and accreditation documents to the WASO.

l. Evaluate and distribute standard automated software security tools to WIN sites to support the WASSO's implementation of this publication.

m. Review and coordinate STPs as described in Chapter I.

n. Evaluate site-submitted software patches for operational effectiveness, security impact, etc.

6. Director, National Security Agency. The Director, NSA, is the National Manager for Telecommunications and Automated Information System Security and performs the following activities that directly relate to telecommunications and INFOSEC for the WIN:

a. Acts as the Federal Government focal point for cryptography, telecommunications systems security, and AIS security.

b. Reviews and approves DOD standards, techniques, systems, and equipment for communications and AIS security.

c. Operates the Information Security Awareness Division of the NCSC to evaluate and certify security of telecommunications systems and AISs.

7. WWMCCS ADP Security Officer. The WASO will:

a. Serve as the primary staff officer to the WIN DAA for matters covered by this publication.

b. Advise, assist, and assess the progress of WIN sites in developing, implementing, and administering effective security programs. The WASO will accomplish these actions through on-site visits, review of documentation, and liaison with parent Service and Defense agency ADP security personnel.

c. Evaluate each WIN site’s security accreditation documentation and make recommendations to the WIN DAA regarding accreditation.

d. Evaluate the mutual security impact of interfaces with other systems (e.g., DSN) and recommend to the WIN DAA a course of action to resolve problem areas.

e. Recommend approval or disapproval to the WIN DAA regarding site-unique software that may affect security.

f. Investigate and resolve security-related issues and incidents involving the WIN, in accordance with Chapter I of this publication.

g. Maintain technical cognizance of all aspects of security associated with the interconnection of WIN

sites, including hardware, software, COMSEC, EMSEC, and other related technical considerations.

h. Maintain this publication and publish amendments and changes as approved by the Joint Staff.

i. Provide liaison with the NCSC for WIN-related security issues.

j. Chair or attend periodic security meetings with other DOD security representatives.

8. Multiuser Host and RNP DAA. In addition to the responsibilities assigned in DOD Directives 5200.28 and 5200.28-M, the DAA (multiuser host and RNP) will:

a. Perform accreditation duties as described in Chapter V and highlighted in Appendix F.

b. Appoint WASSOs and ensure they have the responsibility, authority, training, and staffing to carry out their duties.

c. Ensure that his or her WIN site meets and maintains security requirements prescribed by this publication.

d. Understand that accreditation of the multiuser host or RNP is contingent on results of recurring reviews, testing, and favorable evaluations of security features of the system. Subordinate organizations may be assigned responsibility to implement WIN site security policy and testing and evaluation of security features of WIN elements under their jurisdiction.

9. WWMCCS ADP System Security Manager. A multiuser host DAA may wish to appoint a WASSM for a single site or combination of sites. A detailed description of WASSM responsibilities is included in Chapter IV.

10. WWMCCS ADP System Security Officer. Each WIN multiuser host or RNP site must have a WASSO appointed in writing to implement the requirements of this publication. Detailed responsibilities are given in Chapter IV. AWASSOs may be appointed, in writing, as determined by the command.

11. Terminal Area Certification Authority or DAA. Site DAAs must assign either a Terminal Area Certification Authority or a Terminal Area DAA for each WIN terminal area. The personnel assigned these responsibilities may certify and/or accredit that the terminal area, environment, and equipment meet the requirements of this publication, and in the case of a Terminal Area DAA, will accredit the terminal area for operations. The terminal area certification (and

accreditation if applicable) will be included as part of the WIN multiuser host certification report (Chapter V).

12. WWMCCS ADP Terminal Area Security Officer. Each organization responsible for a terminal area will appoint a WATASO. The WATASO, working in conjunction with the supporting multiuser host WASSO, is responsible for implementing procedures designed to control access to remote devices. The WATASO serves as the primary POC for terminal-related security matters. Detailed responsibilities are given in Chapter IV.

13. WWMCCS Intercomputer Network Director. The WIND will:

a. Coordinate network security-related matters with the WASO.

b. Provide guidance to WIN site coordinators regarding their duties and required interaction with WASSOs.

c. Provide guidance on and monitor the status of continuity of operation plans for WIN components in accordance with Joint Pub 6-03.14, "Operation and Management of the WWMCCS Intercomputer Network."

d. Establish security classification guidance for WIN statistical performance data.

e. Approve JCAT requests from the multiuser host.

f. Approve requests from the multiuser host for group USERID network access.

g. Perform other WIND responsibilities as identified in Joint Pub 6-03.14.

14. Network Operations Center. The NOC will monitor network security and report security incidents to the WASO and the WIND. In this capacity, the NOC will often be the primary liaison between the WASO and WIN sites regarding security incidents.

15. WIN Site Coordinator. The WIN Site Coordinator will:

a. Serve as a WIN multiuser host or RNP focal point for processing site access requests and coordinate with the WASSO on these requests.

b. Remain cognizant of network-related security matters and coordinate with the site WASSO, as required.

c. Review incident reports for WWMCCS-related hardware and software problems as required by Joint Pub 6-03.14.

d. Forward Group USERID (including JCAT) network access requests to WIND for approval.

e. Perform other WSC responsibilities as identified in Joint Pub 6-03.14.

16. Users. Users will:

a. Protect their logon passwords as described in Chapter XII, paragraph 2. Users should change their passwords immediately upon receipt from their WASSO or WATASO.

b. Protect classified and other sensitive materials as specified in Chapter XVI. In particular, users will:

(1) Not leave active computer terminals unattended.

(2) Review system output, including continuity of page numbering.

(3) Ensure that output products, including copies of CRT displays, are appropriately marked and initiate formal accountability for TOP SECRET documents as required by Chapter XVI.

(4) Appropriately mark ADP storage devices TOP SECRET (unless they have been downgraded) and maintain an inventory of ADP storage devices in the user's custody. See Chapter XVI for details.

(5) Follow restrictions on the copying and use of copyrighted and licensed software. In particular, the user will not make copies for private use or use software outside the license agreement.

(6) Give file permissions based on the least privilege concept. (See Glossary.)

c. Report security-related discrepancies. Elements or components of an ADP system will function in a cohesive, identifiable, predictable, and reliable manner so that malfunctions can be detected and reported in time to prevent or minimize disruption of the system. Accordingly, the user will report security-related discrepancies to the WASSO or to the WASSO's designated representative; e.g., WATASO.

CHAPTER III

WIN SITE SECURITY, AIS INTERFACES, AND LANs

1. WIN Site

a. A WIN site may consist of several physical facilities, each containing various SDN-approved hardware, software, and communications elements. The facilities may be interconnected by various communications devices, and the site may have one or more communication connections to other WIN sites or non-WIN systems. Depending on the particular mix of ADP equipment, communications devices, and the sensitivity of information present in a particular facility, the security requirements may vary over a wide range. Because the possible combinations of equipment and environments are large, this section will provide guidelines for categorizing WIN elements so that only a representative number of cases need be considered.

b. WIN computers are considered as members of one of the groups below:

(1) Multiuser Host Computer. A computer with a multiprocessing operating system that performs processing for more than one user simultaneously. The DPS-8000 is an example of a multiuser host. A WIN site can consist of one multiuser host or several hosts, depending on the site mission, organization, and facility.

(2) Single User Intelligent Workstation. A computer that can perform processing for only one user at a time. An intelligent workstation, it can operate cooperatively with a multiuser host or it may operate independently. It may be operated by many users, but never more than one at a time. An example is a workstation with a single tasking operating system, such as a Zenith 248 or WIS CUC running MS-DOS.

(3) Multiuser Intelligent Workstation. A computer that is capable of supporting multiple users simultaneously. An example is a workstation with a multitasking operating system, such as the WIS Workstation (HFSI Macintosh).

(4) LAN Management Processor. A computer that may be a multiuser host or a single or multiuser intelligent workstation. Its function includes administrative support of LAN operations and security. Examples include file and audit servers.

Access to this computer is limited to LAN administrators and security personnel.

c. Hardware devices that are not computers (e.g., printers, terminal servers, or protocol translators) may be connected to the WIN computer types listed above if approved by SDN.

2. WIN Security Mode. DOD Directive 5200.28 defines four security modes of operation for classified AISs. They are dedicated, system-high, partitioned, and multilevel. Each is defined in the Glossary of this publication. The WIN operates in the system-high security mode at the TOP SECRET classification level; i.e., it is a TOP SECRET system-high AIS.

3. WIN-AIS Interfaces

a. General. LANs, video conferencing systems, database machines, multimedia systems, etc., are examples of AISs that may require connection to the WIN. Because the WIN operates in a TOP SECRET system-high mode, AISs connected to the WIN will be accredited to operate at US TOP SECRET. Requests for exception will comply with the following requirements:

(1) Connecting to AISs Accredited Below US TOP SECRET. The SDN requesting approval for connection of the AIS to the WIN will show that WIN data passed to the AIS have been reliably downgraded to the classification level at which that AIS is accredited. Access to the WIN from this AIS is prohibited; i.e., users on the AIS will not be allowed to log on to the WIN.

(2) Connecting to AISs Accredited to Operate in the Multilevel Mode. If the connected AIS is accredited to operate at US TOP SECRET and at one or more classification levels less sensitive than US TOP SECRET, SDN-approved hardware or software or procedures will be in place to ensure that only users with a US TOP SECRET clearance and that have been granted formal access to the WIN can access the WIN. Workstations accredited to operate in the MLS mode will comply with the security policy requirements of Joint Pub 6-03.7 during those periods when they are used for WIN connectivity. If the connected AIS is accredited to operate with SCI, the SDN requesting approval of the connection will show that data from the AIS transferred to the WIN are sanitized of all SCI.

b. SDN Requirement. All connections of AISs to the WIN will be preapproved by SDN in accordance with Joint Pubs 6-03.7 and 6-03.11. SDNs requesting connection of an AIS to the WIN require the following for approval:

(1) Accreditation. The AIS will be accredited by its DAA in accordance with DODD 5200.28 and implementing Service regulations. The SDN will include copies of the accreditation letters from the AIS's DAA and the WIN multiuser host DAA to which it will be connected.

(2) MOA. An MOA will be signed by the WIN multiuser host DAA (or the WIN DAA if the AIS connects directly to the WIN through a PSN) and the DAA of the AIS to be connected. In addition to documenting the interconnection and security requirements, the MOA serves as the formal vehicle for accepting security risks and agreed upon safeguards associated with the connection. If the two DAAs involved are the same person, the MOA becomes an MOR and will be signed only once. The MOA, at a minimum, will include a description of the AISs to be connected, interface requirements, responsibilities, life-cycle management, and COOP. Appendix J provides an outline and list of the minimum requirements to be addressed by the MOA.

(3) Other Requirements. If an MLS Guard is required, a risk index will be calculated in accordance with DODD 5200.28, Enclosure (4), and will serve as a basis from which the guard's security requirements and specifications are derived. Documentation must accompany the SDN to support and validate all aspects of the system's security function. The exact documents will depend on the specific guard and will be determined jointly by the DAAs signing the MOA and approved by the WIN DAA. Normally, the following documents should be included:

(a) Security Policy for the Guard. This document defines the security policy for the guard.

(b) Guard Certification Test. This document identifies those operational and security features and components that must be tested to certify the correct function and operation of the guard. It will include provisions for penetration testing. It further reports the results of certification testing and serves as the basis for determining the adequacy and

correctness of the guard's technical security measures.

(c) Guard Integrated System Test. This document identifies the tests necessary to validate the correct function of the guard installed in its environment. It further reports the results of the Integrated Systems Test for the Guard.

c. Record Keeping. Once approved, all documents associated with the SDN will be filed with the WIN multiuser host's current accreditation documentation. Reaccreditation as a separate action will not normally be necessary because approval of the SDN implies confirmation of current accreditation status. If connection of the AIS is accompanied by a significant reconfiguration of the WIN host system, reaccreditation of the WIN host in the new proposed configuration will normally be a precondition to SDN approval.

4. LANs. A LAN is a specialized AIS that may require connection to the WIN. LANs are classified, insofar as the WIN is concerned, as either WIN or non-WIN. A WIN LAN requires connection to the WIN and has as its primary purpose a requirement to run some WIN standard software; e.g., JOPES. A non-WIN LAN has a primary purpose other than running WIN standard software.

a. WIN LANs. Connection of WIN LANs to the WIN will be approved by SDN in accordance with Joint Pub 6-03.11 before connection. The Services may submit an SDN for approval as a standard LAN configuration. The Joint Staff will evaluate the SDN and, if approved, will delegate approval authority to an appropriate level for additional procurement of like configured LANs. Deviations to the standard configuration must be approved by the Joint Staff. In the event a WIN LAN falls under the authority of a DOD component different from that of the multiuser host, there may be conflicting security policy requirements. To resolve any conflicts, an MOA should be prepared and signed by both DAAs.

b. Non-WIN LANs. Security for non-WIN LANs will be addressed in the MOA between the WIN multiuser host DAA and the DAA of the non-WIN LAN. Connection requirements are listed in paragraph 3 of this chapter.

5. WIN LAN SDN Requirements. All connections of WIN LANs to the WIN multiuser host will be preapproved by SDN in accordance with Joint Pub 6-03.11. SDNs requesting connection require the following for approval:

a. LAN Accreditation. The LAN will be accredited by its DAA to process collateral TOP SECRET information. The SDN will include a copy of the accreditation letter. Furthermore, the SDN will show that the LAN possesses, at a minimum, the functionality of a C2-evaluated system.

b. Risk Analysis. The SDN will include a Risk Analysis of the LAN and interface to the WIN to show that necessary safeguards have been sufficiently tested to assure they provide an acceptable level of trust to the DAAs concerned.

c. The SDN will contain the following documents:

(1) Network Security Architecture. This document will describe the LAN's system security components (hardware, software, and firmware) and services and their function. It will address, in particular, how these components function together with WIN host security features to achieve the required level of system security. (Preparers of this document should consult NCSC-TG-011, "TRUSTED NETWORK INTERPRETATION ENVIRONMENTS GUIDELINE--Guidance for Applying the Trusted Network Interpretation." Network Security Architecture documents will be evaluated against the NCSC-TG-011 for completeness.) Furthermore, this document will contain a table showing the comparison of the LAN's security features and services against the C2 security evaluation class.

(2) Security Concept of Operations. This document will describe how the LAN components can be managed securely to provide the required level of trust.

(3) Test Plan and Report. This document will describe the plan, procedures, and results associated with testing used to validate the function of the security components and services of the LAN both individually and as they combine with those of the WIN multiuser host.

d. MOA. If a WIN LAN is to be connected to a WIN multiuser host under the authority of a different Service with different security requirements than the multiuser host, an MOA between the LAN and host DAAs will be included that resolves any conflicts between the applicable security policies.

6. General Requirements for WIN LANs

a. Accreditation. WIN LANs will have a DAA appointed in writing and will be accredited by the DAA to process

collateral TOP SECRET information independently of the WIN multiuser host to which it is attached. WIN LANs will, at a minimum, possess the functionality of a C2 TCSEC AIS.

b. Identification and Authentication

(1) LAN Users. Each LAN user will be uniquely identified and authenticated at initial logon to his or her workstation. In addition, each LAN user will be uniquely identified and authenticated to all LAN resources to which he or she has access either by the resource or through a controlling processor that mediates access to the resource. Authentication of LAN users will be accomplished by means of passwords unless an alternate method has been approved by SDN as stated in Chapter XII of this publication. Passwords used on WIN LAN resources will be classified as SECRET, the same as passwords on multiuser hosts. Password management will be exercised in accordance with the policy stated in Chapter XII of this publication. The same password may be used to gain access to all resources on a single LAN or group of LAN segments bridged together. WASSOs will determine the extent to which this privilege is extended.

(2) LAN Resources. All LAN resources will be uniquely identifiable to all other LAN resources either directly or indirectly through a controlling processor.

(3) Group USERIDs. Group USERIDs may be used on WIN LANs if it can be shown that they are necessary to achieve an operational capability not otherwise achievable and can be implemented without losing individual accountability. In addition, the policy on Group USERIDs set forth in Chapter XII of this publication is applicable.

c. Access to LAN Resources. Access controls to LAN resources (workstations, servers, hosts, intelligent hubs, etc.) will be administered by the LAN Security Manager. Implementation of access controls may be at the resource or may be achieved remotely using a central Network Management Processor (server). Being a LAN resource, the cable plant or communications subsystem will be accessed, used, and protected in accordance with DODDs C5200.5 and C5200.19.

d. Audit. Audit will be used to detect and deter penetration of a LAN and to reveal usage that identifies misuse. Accordingly, users as well as system and

security administrator actions will be open to scrutiny by means of audit. Audit's purpose relates to the requirement for individual accountability as specified in the DOD 5200.28-STD (Orange Book) Accountability Control Objective, which states:

"Systems that are used to process or handle classified or other sensitive information must assure individual accountability whenever either a mandatory or discretionary security policy is invoked. Furthermore, to assure accountability the capability must exist for an authorized and competent agent to access and evaluate accountability information by a secure means, within a reasonable amount of time and without undue difficulty."

e. LAN Audit Requirement. Audit data will be selectively acquired based on the auditing needs of the particular installation or application. (The need will be determined by the LAN Security Manager.) However, there must be the capability for sufficient detail in the audit data to support tracing the auditable events to a specific individual who has taken the actions or on whose behalf the actions were taken.

f. Required Audit Capabilities. Audit mechanisms on WIN LANs will be capable of meeting the audit requirements specified by DOD 5200.28-STD for the C2 criteria class. Specifically, the audit mechanism will be capable of selectively auditing the following events:

(1) Use of identification and authentication mechanisms.

(2) Introduction of objects into a user's address space.

(3) Deletion of objects from a user's address space.

(4) Action taken by computer operators and system administrators or system security administrators.

(5) Occurrence of all security-relevant events. (See Glossary for definition of a security-relevant event.)

(6) Production of printed output.

g. Auditable Information. The audit mechanism will be capable of recording the following audit information:

(1) Date and time of the event.

(2) Unique identifier on whose behalf the subject generating the event was operating.

(3) Type of event.

(4) Success or failure of the event.

(5) Origin of the request for identification and authentication events.

(6) Name of the object introduced, accessed, or deleted from a user's address space.

(7) Description of modifications made by the system administrator to the user or system security databases.

h. Minimum LAN Audit Requirements. At a minimum, the following events will be audited:

(1) Startup and shutdown.

(2) Logon and logoff.

(3) Object create, modify, or delete.

i. Security of the Audit Mechanism. The audit mechanism will be secure from user or unauthorized manipulation.

j. Centralized Collection of Audit Data. LAN audit data may be generated in a distributed fashion, but it ultimately should be collected, merged, reduced, and evaluated in a central audit server.

k. Other LAN Requirements. Physical, personnel, and communications security requirements for WIN LANs will be consistent with their respective WIN multiuser host requirements in this publication.

CHAPTER IV

WIN SITE SECURITY ADMINISTRATION

1. General. WIN site security administration is the application of INFOSEC policy and guidance to the operation of the WIN. This administration is performed by the WASO, WASSMs, multiuser host and RNP WASSOs, WATASOs, LAN security managers, and users. Because of the need for close coordination between the Joint Staff and WIN site security personnel, frequent and direct contact is required.

2. WWMCCS ADP System Security Manager. A WASSM may be charged with security responsibilities for multiple WWMCCS and non-WWMCCS ADP systems. The WASSM would normally concentrate on security policy issues and is assisted in policy implementation by WASSOs and other support personnel. At a minimum, the WASSM's responsibilities will include:

   a. Providing general supervision, administration, and overall coordination of WIN security matters, including analysis, test, evaluation, certification, and accreditation.

   b. Ensuring that security instructions, guidance, and standard operating procedures are prepared, issued, and maintained for the WIN site.

   c. Monitoring implementation of such instructions and procedures and directing action appropriate to remedy security deficiencies.

3. WWMCCS ADP System Security Officer

   a. Appointment. A WASSO for each multiuser host or combination of hosts at a WIN site will be appointed in writing by the appropriate site or multiuser host DAA or by the DAA's designated representative. The WASO and all WIN multiuser host sites will be notified of the WASSO's appointment. AWASSOs may be appointed as required.

   b. Privileges. WASSOs and AWASSOs will not normally have unrestricted access to all data on their respective multiuser hosts. Access will be limited to that required to accomplish their duties. Access beyond that normally required will be granted on a case-by-case basis by the DAA to accomplish specific tasks; e.g., conducting an investigation. The access will be granted in writing by the DAA and will be limited to the time necessary to accomplish the specific task for which it is granted. An

expiration date will be included in the letter granting the access.

c. Organizational Relationships. The operational objectives of maximum throughput and minimum response time may conflict with the security objectives of maximum control and minimum risk. In this regard, having a WASSO or AWASSO work for an operational element such as Computer Operations or Systems Software is considered a security risk and is discouraged. The WASSO should have direct access to the multiuser host and RNP site DAAs. Ideally, the WASSO should work directly for his or her respective DAA.

d. WASSO Qualifications. The WASSO or AWASSO will be a US Government employee who is technically capable of ensuring that WIN security policy and guidance in this publication and other directives have been properly implemented. At a minimum, the WASSO's personal technical qualifications or the technical qualifications represented by available site personnel directly supporting the WASSO's security functions will include:

(1) Experience in computer operations on a WIN multiuser host computer or equivalent.

(2) Completion of a basic INFOSEC course of instruction.

(3) Completion of a WIN-specific security course of instruction.

(4) Completion of a system software programmer's course for a WIN computer system.

(5) Experience as a system software analyst or programmer on a WIN multiuser host computer or equivalent.

(6) Experience in the application and enforcement of information and ADP security measures and countermeasures to security threats and vulnerabilities.

e. WASSO Responsibilities. Within the framework of published security policy, the security measures for WIN multiuser host site facilities and related areas (e.g., LANs, remote terminal areas, etc.) will be prescribed by the WASSO and approved by his or her respective DAA. The WASSO will be the focal point for WIN site security matters. WASSO responsibilities will be defined by the appropriate command authority, who will consider the

following items a minimum baseline when assigning WASSO duties:

(1) Develop, review, revise, and submit for approval procedures for reporting, investigating, and resolving WIN security incidents involving the site.

(2) Ensure that personnel who install, operate, maintain, or use the WIN hold the proper security clearance and access authorization and are indoctrinated by their respective security officer in applicable security requirements and responsibilities.

(3) Supervise review of security audit information. (Refer to Chapter XII, paragraph 5.)

(4) Develop, review, revise, submit for approval, and implement procedures for monitoring and reacting to security warning messages and reports.

(5) Formulate procedures to implement physical, administrative, and personnel access controls for WIN computers.

(6) Participate in system malfunction analysis and in the preparation of security incident reports.

(7) Evaluate site software patches made to WIN standard operating system software to ensure that they do not create security vulnerabilities. If in doubt, submit the patch to DISA for evaluation.

(8) Evaluate the effectiveness and impact of security measures and procedures regarding connection of WIN site elements and other systems (e.g., DSN). Assist in preparing SDNs and SCPs. If necessary, prepare correspondence to the appropriate command authority or DAA identifying problem areas, as appropriate.

(9) Report security incidents that could damage network security to the appropriate command authority or DAA for consideration and appropriate action; e.g., compliance with the Computer Security Technical Vulnerability Reporting Program prescribed by DODI 5215.2.

(10) Immediately notify the appropriate command authority or DAA of suspected security incidents associated with a subordinate network site. Provide recommendations to assist the DAA in determining if

other sites should be denied access to resources at the site having the problem and if network access should be denied to that site. The WASSO will be notified of actions taken by the command or DAA.

(11) Prepare necessary directives that implement WIN or site DAA prescribed security measures to be used at each site installation and monitor their application.

(12) Maintain documentation detailing site hardware and software configuration and countermeasures that protect the site from threats.

(13) Ensure that inspections are conducted as required by this publication or applicable Service or Defense agency directives.

(14) Maintain files on current Risk Analysis with Accreditation letters and related documentation. Included will be all waiver-related documentation.

(15) Conduct system audits, verifications, and acceptance checks and maintain documentation on the results.

(16) Conduct random audits to verify compliance with security procedures and requirements of this publication.

(17) Evaluate the security impact of proposed site-unique modifications to operating system software and recommend approval for those that do not adversely affect security. Request prior approval from the WIN DAA for site-unique modifications to software that affect other WIN sites.

NOTE: These modifications are limited to those necessary to configure the operating system to a particular WIN site.

(18) Periodically monitor system use. With the DAA’s authorization, inspect and monitor user files for possible security problems.

(19) Represent the site at meetings concerning WIN security.

(20) Coordinate STPs.

(21) Perform WASSM-related duties when a WASSM is not appointed.

(22) Review security impact of SDNs or SCPs in accordance with Joint Pub 6-03.11 before their submission for approval. Prepare and sign a separate statement of review as part of the SDN or SCP submission.

(23) Identify security requirements and manage access in relationship to remote AISs that afford multiuser connections into the WIN.

4. WWMCCS ADP Terminal Area Security Officer

a. General. A WATASO is responsible for implementing security for remote terminals and peripheral devices. The security measures for a peripheral device or remote terminal and the adjacent area will be prescribed by the WASSO and approved by the multiuser host DAA.

b. Appointment. The organization responsible for the terminal area will appoint in writing a WATASO who will control access to the remote device(s) and will serve as the WASSO's single point of contact for that terminal area. The WATASO will have direct access to the terminal area certification authority or DAA. The WATASO will be a WIN user.

c. WATASO Qualifications. The WATASO will be a US Government employee who is technically capable of ensuring that WIN security policy and guidance in this publication and other directives have been properly implemented. At a minimum, the WATASO'S personal technical qualifications will include:

(1) Experience in computer operations on a stand-alone workstation, minicomputer, or mainframe computer.

(2) Completion of a basic INFOSEC course of instruction.

(3) Completion of a WIN-specific security course of instruction.

(4) If responsible for multiuser intelligent workstations, the WATASO must have attended a system administrator's course of instruction for that workstation.

d. WATASO Responsibilities. A WATASO will be appointed for each terminal area and will implement procedures to control access to remote devices. WATASO duties will include:

(1) Assisting the WASSO in preparing terminal security procedures.

(2) Implementing approved security procedures.

(3) Maintaining a current access list of personnel authorized access to the remote device(s).

(4) Reporting security abnormalities to the WASSO or a designated representative.

(5) Safeguarding and returning to the WASSO or a designated representative ADP products that cannot be identified or that contain extraneous data; i.e., unrequested data.

(6) Conducting random audits to ensure that security procedures and requirements of this publication for the terminal area are being followed.

(7) Issuing the initial password to approved users of workstations requiring workstation logon passwords in addition to multiuser host logon passwords.

(8) Maintaining and reviewing appropriate audit files residing on workstations with audit capabilities.

(9) Serving as the workstation administrator for intelligent workstations within his or her terminal area.

5. LAN Security Manager

a. Appointment. If a WIN LAN is connected to a WIN multiuser host, the host DAA will appoint in writing a LAN Security Manager whose primary duty will be to monitor and control security aspects of the LAN's operation. The LAN Security Manager will have direct access to the LAN DAA.

b. Qualifications. The LAN Security Manager will be a US Government employee who is technically capable of ensuring that WIN security policy and guidance in this publication and other directives have been properly implemented on the LAN. The LAN Security Manager's personal technical qualifications or the technical qualifications represented by available site personnel directly supporting the LAN Security Manager's security functions will be equivalent to the qualifications of a WASSO. In addition, the LAN Security Manager will have

completed a LAN administrator's course for the LAN being managed.

c. Duties. The LAN Security Manager's duties will include:

(1) Preparing LAN security procedures.

(2) Implementing approved LAN security procedures.

(3) Establishing LAN user accounts.

(4) Managing LAN user accounts and passwords.

(5) Maintaining LAN access controls.

(6) Conducting random audits to ensure that security procedures and requirements of this publication for the LAN are being followed.

(7) Performing routine security functions; e.g., denying access based on security violations.

(8) Analyzing LAN audit reports.

(9) Ensuring correct function of LAN backups.

(INTENTIONALLY BLANK)

CHAPTER V

ACCREDITATION, CERTIFICATION, AND RISK MANAGEMENT

1. Accreditation

a. Accreditation is a formal declaration by the DAA that an AIS or network is approved to operate:

(1) In a specific security mode.

(2) With a prescribed set of administrative, environmental, and technical security safeguards.

(3) Against defined threats with stated vulnerabilities and countermeasures.

(4) In a given operational environment.

(5) Under a stated operational concept.

(6) With stated interconnections to other AISs or networks.

(7) At an acceptable level of risk for which the accrediting authority (DAA) has formally assumed responsibility.

b. Accrediting Authority. The accrediting authority is the DAA. The DAA formally accepts security responsibility for the operation of an AIS or network and officially declares that it will adequately protect classified information against compromise, destruction, unauthorized alteration, or denial of service through the continuous employment of safeguards including administrative, procedural, physical, personnel, communications security, emanations security, and computer-based (e.g., hardware, firmware, software) controls. In the WIN, the accreditation statement affixes security responsibility with the DAA and shows that security has been addressed in accordance with this publication. The DAA must be at an organizational level, have authority to evaluate the overall mission requirements, and provide definitive directions to developers in order to adequately address risk in their system. The DAA will be appointed in writing.

c. Risk Analysis. The accreditation decision is based on results of the certification and accreditation process that focuses on a Risk Analysis. The Risk Analysis enables the certification authority to make informed decisions on system security deficiencies and actions needed to correct those deficiencies. The Risk

Analysis integrates all the pieces of the certification process, ensuring that each piece of the system is appropriate and that overall, the security posture of the system is acceptable.

(1) Certification. The end product of a Risk Analysis is certification. Certification is defined by DODD 5200.28 as "the technical evaluation of an AIS's security features and other safeguards, made in support of the accreditation process, which establishes the extent that a particular AIS design and implementation meet a set of specified security requirements." Upon completion of certification, the Risk Analysis Report is produced and presented to the DAA as the basis for accreditation.

(2) ST&E. An important part of certification is the ST&E, which is used to examine, analyze, and report on security countermeasures and safeguards as they have been applied in an operational environment. The ST&E provides factual evidence and documentation on the effectiveness of implemented countermeasures. The ST&E is a major part of the Risk Analysis Report.

d. Accreditation

(1) The completed Risk Analysis with an ST&E is the document on which the DAA bases his or her accreditation decision. Ultimately, the decision to accredit an AIS reflects the DAA's judgment to operate the system after weighing the system's risks against the operational need for the AIS.

(2) Each WIN multiuser host and connecting AIS (RNPs, LANs, etc.) will be accredited for stand-alone operations. Furthermore, each WIN multiuser host will be accredited to operate in the WIN; i.e., the host's connection to the WIN will be accredited by the WIN DAA. The certification and accreditation process for both stand-alone operations and connection to the WIN will be repeated on a triennial basis.

2. Accreditation Requirements for Stand-Alone Operations

a. Multiuser Hosts. Each multiuser host DAA will accredit his or her host for stand-alone operations upon completion of a review of the site's Risk Analysis (See Appendix E) and acceptance of the AIS's residual risks. The review will include not only the host's site Risk Analysis, but those for all AISs connected. Each AIS's connection to the host must be accredited by the

multiuser host DAA before the host can be accredited for stand-alone operations.

b. Connected AISs (RNPs/LANs/Remote DATANET-8s/Concentrator and Terminal Areas). Each connected AIS's DAA will accredit his or her AIS for stand-alone operations upon completion of a review of the site's Risk Analysis and acceptance of the AIS's residual risks. Host DAAs will decide which terminal areas need Terminal Area DAAs.

3. Accreditation Requirements for Connection to the WIN

a. Interim Connections. Interim connections may be granted by the WIN DAA for no longer than 6 months. The local DAA will send a request to the WIN DAA stating that the following minimum security safeguards have been met:

(1) Physical security of WIN components meets the requirements of Chapter VIII of this publication.

(2) WIN users possess an interim or final US TOP SECRET clearance.

(3) A WASSO and WATASOs have been appointed in writing.

(4) WIN users have been instructed in their responsibilities for protecting their SECRET passwords and the rules for accessing and protecting WIN resources, especially information.

(5) Communications links meet the requirements for transmission of TOP SECRET information.

b. Final Accreditation. The Risk Analysis will be used as the basis for requesting final accreditation for connectivity to the WIN. Final accreditation will be valid for a period of 3 years unless a major change is made to the multiuser host, in which case a resubmission of the Risk Analysis is required.

NOTE: A "major change" is a change such as a site relocation, major facility modification, complete change in multiuser host operating system, or connection of a WIN or non-WIN network or AIS to the WIN.)

Requests for final accreditation will comply with the following:

(1) Multiuser Host Connections to the WIN. For multiuser host connections to the WIN, the request for final accreditation will contain:

(a) Multiuser host DAA accreditation letter for stand-alone operations (see Appendix C).

(b) Multiuser host Risk Analysis.

(c) Accreditation letters from the DAAs of connected AISs along with copies of the respective MOAs, if applicable.

(2) Remote AIS Connections to the WIN. Remote AISs (RNPs, LANs, etc) may connect to the WIN through a multiuser host or directly through a DATANET-8 connected to a PSN. Requests for final accreditation will be handled as follows:

(a) Connected to the WIN through a Multiuser Host. For remote AISs connected to the WIN through a multiuser host, the multiuser host DAA will be the accrediting authority for the connection. The request for final accreditation will contain:

1. Remote AIS accreditation letter for stand-alone operations signed by the remote AIS DAA.

2. Remote AIS Risk Analysis.

3. Accreditation letters from the DAAs of connected AISs along with copies of the respective MOAs, if applicable.

(b) Connected Directly to the WIN. For remote AISs connected directly to the WIN, the WIN DAA will be the accrediting authority for the connection. The request for final accreditation will be submitted through the appropriate chain of command to the WIN DAA, the Joint Staff, J-6. The request for final accreditation will contain:

1. Remote AIS accreditation letter for stand-alone operations signed by the remote AIS DAA.

2. Remote AIS Risk Analysis.

3. Accreditation letters from the DAAs of connected AISs, along with copies of the respective MOAs, if applicable.

c. Amendments. Once a Risk Analysis has been submitted, and final accreditation has been granted, minor additions or deletions of equipment or changes in configuration or procedures do not require resubmission of the entire Risk Analysis for reaccreditation. Instead, an amendment in letter format with necessary enclosures detailing the change will be sufficient. (If the change involves only the addition of equipment, the SDN will serve as the vehicle to accomplish this requirement.) The amendment should thoroughly address the impact it has on the overall risk posture of the multiuser host. The amendment will be submitted through the same chain of command as the Risk Analysis.

4. CINC, Service, or Defense Agency Review

a. CINC Review. WIN organizations (WIN multiuser host sites) in a CINC's theater of operations will send network accreditation requests to the WIN DAA (Director, J-6, Joint Staff) through the CINC and appropriate Service. The CINC may require corrective actions by the submitting organization before sending the request through the appropriate Service to the WIN DAA. In such a case, the CINC will inform the WIN DAA if delays are expected.

b. Service or Defense Agency Review. Accreditation requests sent to the WIN DAA (J-6, Joint Staff) will be sent through the appropriate Service; Defense agency; or Director, Joint Staff, for NMCC systems for review of compliance with applicable Service or Defense agency regulations. Comments will be sent to the WIN DAA with the accreditation request.

5. Risk Management Process. Risk management is an ongoing process that ensures a system's risk posture does not exceed an acceptable level. Risk is a measure of the potential for an AIS to allow unauthorized disclosure of classified or sensitive unclassified information, to permit information integrity loss, or to pose a service denial hazard. Through the risk management process, risks are identified and measured and then minimized or accepted. At a minimum, DAAs will develop and implement a risk management program for their WIN sites that:

(a) Identifies their WIN resources.

(b) Analyzes the risks associated with the potential for espionage, sabotage, damage, penetration, or theft to determine the minimum level of protection required.

(c) Maintains procedures for update, review, and reporting of risks, vulnerabilities, and evaluation of safeguard effectiveness.

(d) Develops and maintains a written plan that identifies actions required to correct or improve risks to an acceptable level.

(INTENTIONALLY BLANK)

CHAPTER VI

ADP SECURITY TRAINING AND AWARENESS

1. Training Program. Each WIN site DAA will establish an INFOSEC training program that stresses safeguarding WIN resources and classified information. The WIN security training and awareness program will address all users and their security-related activities. At a minimum, the program will:

a. Indoctrinate personnel in principles, criteria, and procedures to properly safeguard WIN resources and inform them of the strict prohibitions against disclosure of classified information, fraud, waste, and abuse contained in DOD, Service, and Defense agency regulations.

b. Familiarize personnel with the following:

(1) The risks existing at their location.

(2) The specific WIN security requirements of their DOD Component.

(3) Their specific duty assignments.

c. Inform WIN users of the penalties for violation or disregard of the provisions of this publication.

2. Training Frequency. WIN users will receive the training in paragraph 1 of this chapter, initially, and as frequently as required, by their respective Service regulations. Training will occur at least once every 12 months.

3. Security Personnel Training. The WIN multiuser host DAA will ensure that the site security staff at all levels is adequately trained to perform its security role as required by this publication and applicable DOD, Service, and Defense agency regulations.

(INTENTIONALLY BLANK)

CHAPTER VII

PERSONNEL SECURITY

1. Clearance. Personnel who have unescorted access to TOP SECRET WIN areas will have an interim or final US TOP SECRET clearance. In addition, personnel requiring access to WIN information will have been granted access to the WIN based upon a need to know for specific data on the WIN. Personnel who do not possess the proper clearance will be escorted by properly cleared personnel while in a WIN area.

2. Contractors

   a. Contractors who have WIN access will have the same clearance and need-to-know as other WIN users. Contractor personnel requiring access to TPFDD data must be approved for that access in accordance with CJCS MOP 60.

   b. Contractors who maintain hardware connected to the WIN will possess a US TOP SECRET clearance or be escorted.

   c. Contractor maintenance visits to WIN areas will be recorded and retained for 24 months. This requirement does not apply to contractor maintenance personnel who are assigned on site.

   d. Contractors will not serve as WASSMs, WASSOs, WATASOs, WSCs, TP8 Administrators, or LAN Security Managers and will not be given administrator privileges.

   NOTE: This requirement is waiverable by the multiuser host DAA. As with other site waivers, it must be reported in the site's triennial Risk Analysis.

3. Two-Person Staffing. Because of the extreme importance to national security of TOP SECRET information, and for safety reasons, all WIN areas that require staffing will be staffed by at least two appropriately cleared persons. (See Appendix F.)

4. Foreign Nationals. Foreign nationals will not have access to WIN software or data resources as users or maintenance personnel without the WIN DAA approval. Foreign nationals will not install, repair, or maintain WIN hardware. Foreign nationals will not serve as WASSMs, WASSOs, WATASOs, WSCs, TP8 Administrators, or LAN Security Managers.

5. Escort Requirements. Escorts will be technically competent and will ensure that visitors or non TOP SECRET cleared maintenance personnel do nothing that might degrade

or circumvent implemented security countermeasures or safeguards in WIN facilities or equipment. Harmful or questionable actions taken by these personnel will be reported immediately to the security officer (WASSM, WASSO, or WATASO). Escorts will alert other personnel whenever an escorted person is in their area. Escorts will ensure that terminal screens or other devices are protected from casual observation by visitors.

6. Personnel Problems. Managers at all levels must monitor their WIN users and support personnel for indications of instability that might pose a threat to WIN resources. Temporary removal of WIN access pending an official evaluation may be appropriate in some cases. DOD 5200.2-R contains amplifying guidance in this area.

7. Dismissed and Departed Personnel

a. WIN users who are to be dismissed from a WIN access position under unfavorable circumstances will be denied all WIN access privileges immediately. These personnel are historically among the greatest threats to automated systems. The revocation will be accomplished before notifying the person whose access will be terminated. The commander of the organization of the dismissed or departed WIN user will ensure that the WASSO or WATASO are notified.

b. Upon notification that a WIN user’s access will be terminated, the following actions will be accomplished:

(1) The WASSO or designatee will delete the WIN user’s multiuser host or RNP system access permissions.

(2) For workstations with logon passwords, the WATASO will delete the WIN user’s access to the workstation.

(3) Physical access to the WIN areas will be removed.

(INTENTIONALLY BLANK)

CHAPTER VIII

PHYSICAL AND ENVIRONMENTAL SECURITY

1. Physical Security Principles. Physical security of WIN information is based upon the requirement that TOP SECRET information will be protected at the TOP SECRET level. DOD 5200.1-R provides guidance for protection of TOP SECRET information. In the WIN environment, physical security principles are derived from guidance in DOD 5200.1-R as follows:

   a. Physical security will be provided through an in-depth application of barriers and procedures including continuous surveillance (human or electronic) of the protected area and equipment.

   b. Disasters such as fire and floods will be prevented, controlled, or minimized to the extent economically feasible by using detection equipment, fire extinguishing systems, and tested emergency measures.

   c. Trained physical security specialists will be relied on to provide specific guidance on physical security requirements and safeguards in accordance with this publication and applicable DOD, Service, and Defense agency regulations.

2. Multiuser Host Processor Areas. Physical security for multiuser host processor areas will satisfy TOP SECRET open storage requirements of the DOD component concerned.

3. RNP/Remote DATANET-8/Concentrator/LAN Sites and Terminal Areas. Physical security of WIN RNP, remote DATANET-8/ Concentrator/LAN sites and terminal areas will be provided either by one of the following:

   a. Twenty-four-hour staffing by US TOP SECRET cleared personnel who are listed on the facility’s access roster.

   b. A Class A or B vault that meets the standards established by the head of the DOD component concerned.

   c. A US Government controlled access area with entrances and emergency exits alarmed and with motion detectors designed to detect unauthorized entry. This area must be considered by the local responsible official to provide equivalent or better protection than subparagraphs 3a or 3b above. The physical barrier will be such that forcible attack will give evidence of attempted entry into the area. The alarm will, at a minimum, provide immediate notice of attempted

unauthorized entry to a continually staffed, US Government or US Government contracted security force. Clearance level requirements for the security guard personnel will be determined by the multiuser host DAA in coordination with the base commander. The security force must be capable of responding to an alarm in no more than 10 minutes. Classified workstation magnetic media may be stored in the workstation during nonduty hours (no personnel present) in this type of area. However, depending on the terminal area's location (e.g., overseas sites), DAAs may require that classified workstation removable magnetic media be removed and stored in a GSA-approved security container approved for storage of TOP SECRET information during nonduty hours. Storage of the classified magnetic media in the workstation as described above is appropriate only under ideal conditions where the threat level is low.

4. Securable Containers as Remote Terminal Areas. Specially designed containers for ADP equipment have been developed that meet the requirements of subparagraph VIII-3c above and may be used as remote terminal areas. Such containers will be reviewed by the WASSO and approved by the local DAA before use. In addition, sites using securable containers will develop and indoctrinate users on operational procedures associated with their use. Furthermore, users of securable containers will observe the following precautions:

a. When in use, a physical control zone (controlled space) around the WIN workstation or terminal will be established to prevent access or viewing by unauthorized personnel.

b. TEMPEST countermeasures will be determined in accordance with NTISSI 7000 and implementing Service regulations.

c. If the area or room in which the securable container is used does not meet the conditions of paragraph 3 above, the encryption device (e.g., STU-III) used with the WIN workstation or terminal will be physically located inside the same securable container as the WIN workstation or terminal. In addition, no communication lines connecting the workstation or terminal to the encryption device will be allowed to run outside the securable container.

d. When not in use, cryptographic keying material will be safeguarded in accordance with published DOD COMSEC policies and procedures.

5. Protection of WIN Hardware. To guard against sabotage or bugging, hardware to be connected to the WIN will be protected at the TOP SECRET level. This hardware will be protected by one of the following methods:

a. Stored in a TOP SECRET area.

b. If TOP SECRET level protection is not achievable, WIN hardware must first be downgraded by removing all WIN data storage media and stored in a TOP SECRET area. For storage in a non-TOP SECRET area, hardware will be protected in such a way that tampering with internal parts is recognizable. In particular, the following precautions are required:

(1) The non-TOP SECRET area in which equipment is located must be lockable and must not provide opportunity for reconnection of the hardware to the WIN without WASSO action.

(2) For added indication of tampering or bugging, NSA approved tamper-indicative seals may be used at the site DAA's discretion. If used, the site will develop local procedures for using and tracking the lifecycle of the seals.

(3) If, for any reason, a seal has been removed or appears to have been tampered with, it will be assumed that the WIN hardware has been tampered with or bugged. A TSCM inspection of this hardware will be performed prior to reconnection to the WIN.

NOTE: This policy does not diminish the WIN site user's responsibilities and accountability for protecting WIN resources when using NSA's tamper-indicative seals.

6. Protection of Supporting Utilities. ADP operations of a WIN component, especially a multiuser host, depend on supporting utilities. These include electric power, air-conditioning, communications circuits, fuel supplies, and water. All site DAAs should consider local threats and provide suitable protection to these utilities insofar as possible. Uninterruptable power supplies, auxiliary power generators, power distribution panels, power filters, and air handling units should also be considered.

(INTENTIONALLY BLANK)

CHAPTER IX

SOFTWARE SECURITY

1. Introduction. The software security policies contained in this publication apply to all software used on WIN computers. They prescribe the amount of security protection to be provided by and for that software. The requirements of this chapter must be met by Government-developed software, software developed by contractors, or SDN-approved COTS software. The policies in this chapter, except for paragraph 3, apply primarily to operating systems and application systems software designed to run on WIN multiuser host computers. Software for intelligent workstations is discussed in paragraph 3. If the requirements of this chapter cannot be met, the risk analysis report will so state and appropriate waivers will be requested.

a. Software developed for use on the WIN will have configuration management controls and will be approved through the SDN process in accordance with Joint Pub 6-03.11 to protect against and detect unauthorized alteration.

b. Although most access control mechanisms reside in the operating system or special security packages, security considerations will be included in all levels of software. Software will be thoroughly evaluated to ensure it does not circumvent system security controls.

c. Security will be considered throughout the life-cycle process for software. Security added after the initial development phases is often ineffective and more expensive.

d. User, operator, and programmer documentation will include a description and explanation of software security features to allow for their effective use.

e. Security software features will be included in the IST to ensure proper security protection of system operations. Testing will be thorough, because security controls must protect against both intentional hostile acts and accidents.

2. Firmware. Firmware is software that is permanently stored in a memory device. Firmware can be read by a subject (WIN user) but cannot be written to or modified by a user. The most common memory for firmware is read-only memory and it is usually located on a semiconductor chip. Firmware modifications will follow the approval requirements

of Joint Pub 6-03.11. Firmware may be modified in the following ways:

a. By DISA, as a standard upgrade.

b. By contractor field engineers. Field engineers will notify the WASSO when making a firmware change to other than test and diagnostic equipment.

3. Intelligent Workstation Software. Software used on a WIN-connected intelligent workstation will be either:

a. Joint, Service, or Site Developed. This software is developed by Government or contractor personnel and controlled in accordance with configuration management policy set forth in Joint Pub 6-03.11, as well as applicable Service and Defense agency regulations.

b. COTS Software. COTS applications software may be used on WIN workstations if approved in writing by the WASSO. An SDN is required only if the software interacts with WIN software (e.g., ETC). All data files created or modified using COTS software on the workstation will be considered TOP SECRET until appropriately downgraded in accordance with Chapter XVI of this publication.

NOTE: Users of workstations using MS-DOS as the operating system are cautioned about saving or copying data files to floppy disks. Classified data may be inadvertently copied in the space between the "end of file" marker and the end of a block. This space must be examined before the floppy disk can be downgraded to the target classification.

c. Approved Public Domain Software. Because of risks (such as software viruses) associated with public domain software, its use is unauthorized unless the source code has been approved by the J-6, Joint Staff, through an SDN, in accordance with Joint Pub 6-03.11.

4. Protection of Software. Software developed specifically for use on the WIN will be protected during its development, distribution, and maintenance phases. Protection is required to prevent implanting of software bugs and to ensure the code is not altered.

a. Software Classification. Software will be classified at the highest level of information or aggregation of information that can be derived from the software (See Appendix B). The classified information may be contained in:

(1) Program comments.

(2) Edit criteria, including value of constraints.

(3) Data-field names, descriptions, or tables.

(4) Algorithms or processes.

(5) Aggregation of all or some of the above.

A careful study will be made of software to determine its classification. Software as described in subparagraphs 4a(1) through 4a(5) above will be classified (if appropriate) regardless of how it is stored or represented. However, if the comments alone take it to a higher classification, the object code may have a lower classification if it does not include the comments.

b. Trusted Software. Trusted software will be protected at the highest level of information it processes and placed under configuration control by security personnel to ensure its trustworthiness.

c. Clearance Requirements for Software Developers. Government and contractor personnel who develop, modify, or maintain WIN applications software will possess at least a US SECRET clearance. COTS software is exempt from this requirement unless it is modified for WIN usage.

5. Software Releases. This paragraph pertains to releasing versions of standard software packages; e.g., JOPES, JOPS, JDS, multiuser host operating system by a DDA such as DISA, USTC, and other agencies that serve as DDAs.

a. Development of New Releases

(1) Development and certification of security specifications by the DDA will be coordinated with affected Joint Staff OPRs and validated by the WASO prior to development.

(2) Security specifications should address the ability of the system to withstand penetration efforts (if appropriate) and the functional ability of the system, under normal constraints, to identify, control, and record individual access to the system, and to properly mark ADP products.

(3) Design reviews for new system releases will be conducted by the DDA in coordination with the WASO to ascertain if the proposed design meets approved

specifications. Results of the design review will be fully documented and maintained as official records by the WASO and the DDA.

(4) The DDA will conduct an IST of new system releases to demonstrate the functionality and stability of the new system release. This will ensure that the system meets the approved security specifications and that the new system release does not alter or have a negative impact on existing security policy implementation. The purpose of these tests will be to determine that security features function correctly.

(5) Testing will be conducted on development copies of the software using test data bases. If operational user files are required for testing, only copies of these files will be used. The volume and variety of test data and the extent of testing will be sufficient to ensure that the system will function in a cohesive, identifiable, predictable, and reliable manner. Upon completion of testing, test results will be fully documented, protected, and maintained as part of the official records of the WASO and the DDA. Before release of the system to WIN sites, the DDA will certify to the J-6, Joint Staff, that the system meets documented and approved security specifications, and that results of the test demonstrate adequate security provisions are present and functioning correctly.

b. Distribution of New Releases. Methods provided in NCSC-TG-008 will be used for all software to ensure that products delivered operate under a correct implementation of the security policy of this publication. In particular:

(1) The DDA will forward new releases of systems and applications software to the WASSO at each WIN site through registered mail. (This includes multiuser host operating system software and its utilities, joint mission software running on multiuser hosts, and joint mission software running on workstations.) Operating system updates for workstations should be sent directly to the WATASO or workstation administrator.

(2) Unclassified microfiche and documentation may be sent through first class mail or courier.

(3) The DDA will enclose within each shipment a "shipment received" card to be completed by the WASSO, WATASO, or workstation administrator and

returned to the DDA. Information on the "shipment received" card will include shipment number, name, organization, and address of recipient, as well as date of receipt.

(4) The DDA will additionally notify each site by unclassified message indicating the registry or shipment number as appropriate, method of shipment, and the date such material was forwarded to the site.

c. Site Verification of New Releases. Each multiuser host WASSO will verify the authenticity of software received by comparing the registry or shipment number of the software package with that contained in the message from the originating DDA and return the enclosed "shipment received" card to the DDA. If, after 15 days from the forwarding date, the site has not received the expected software shipment, it will advise the DDA through message so that the DDA may initiate tracer action. Each site will notify the DDA upon implementation of the new software.

d. Virus Screening of COTS. All COTS will be screened for malicious software before installation on WIN computing equipment in accordance with Chapter XIX of this publication.

(INTENTIONALLY BLANK)

CHAPTER X

WIN SITE OPERATING SYSTEM SOFTWARE SECURITY

1. General. All WIN site operating system software will be approved in accordance with Joint Pub 6-03.11 before installation and use on any WIN hardware. Before use, all operating system software will meet the requirements of this chapter. If the requirements of this chapter cannot be met, the Risk Analysis report will so state and appropriate waivers will be obtained.

2. Minimum Requirements for WIN Site Operating Systems Software Configuration Control. The WASSO will maintain a site log of verified operating system changes or site option patches. Modifications to the operating system will be kept under close control and cross-checked by two appropriately cleared system programmers. Modifications impacting functional areas will be coordinated with the local OPR before implementation. The site log will contain at least the date, identification of the operating system release, description of the site option or modification, the exact code (if appropriate), reason for the modification, modules affected, and the names of the responsible operating system programmers who created and cross-checked the modification. The site log of modifications, along with test results and data, will be maintained until at least the next major software release.

a. System Startup Files. A master copy of the system startup file will be maintained in a secure location separate from the WIN multiuser host ADPE and under the control of the WASSO. The startup procedures will be described in the site Trusted Facility Manual to provide a known processing environment. The startup file will be physically protected to ensure that unauthorized access is precluded. The WASSO staff, in coordination with system software personnel, will authenticate system patches by random checks of the patch section in the system startup file. If a password must be embedded in the startup file, the file will be protected at the SECRET level.

b. System Tapes and Disks. System tapes and disks will be uniquely identified and protected at the TOP SECRET level, as well as all restrictive categories of data that the multiuser host is processing or storing on-line. Subject to the WIN multiuser host site DAA’s approval, the WASSO will develop a method to control access to system tapes or disks. Unauthorized requests for system tapes and disks will be reported to the WASSO.

c. System Module Source Listings. System module source listings will be physically protected as FOUO information. Access will be controlled on a need-to-know basis.

3. Minimum Requirements for DISA-Released WIN Site Operating System Software

a. Initial Testing of New Operating System Releases. Before implementing a new system software release, DISA will complete testing sufficient to verify that the system software meets documented and approved security specifications and complies with existing security policy. Deficiencies will be documented and made known to all WASSOs. Initial testing and debugging of new releases should be performed during dedicated time in a controlled environment. Operational testing in a dedicated environment will be conducted with copies of operational files. Testing will include SDN-approved patches and modifications to ensure the integrity of the operating system's security features.

b. Site Testing and Integration of New Operating System Releases. WIN site selectable options included in the DISA operating system release package are customized by the individual multiuser host sites. WIN sites have the authority to modify or develop site-unique operating system modules. Modifications to the standard operating system, as furnished to the WIN sites by DISA through an SRB, will be modified only by DISA or under DISA direction. Site-unique patches that affect operation of the WIN require prior approval of the WIN DAA through an SDN. Startup files will not be updated until the WASSO has verified modifications or patches by testing.

(INTENTIONALLY BLANK)

CHAPTER XI

APPLICATIONS SOFTWARE SECURITY FOR WIN SITES

1. General. The following policy applies to development of WIN sites' applications software with the following characteristics.

a. The software is capable of running on more than one WIN site computer on the WIN.

b. The software can use privileged functions or enter privileged states.

c. The software is capable of changing identity during execution; i.e, it can spawn jobs under a USERID other than the USERID used to execute the program.

2. Development and Testing of WIN Standard and Service-Unique Applications Software

a. Security specifications for each new applications software release will be developed by the DDA, coordinated with the WASO and affected Joint Staff or Service OPRs, and approved by the WIN DAA J-6, Joint Staff, before development of that release.

b. Design reviews for new WIN applications software releases will be conducted by the DDA to ensure that proposed designs meet approved specifications and do not conflict with existing WIN security policy. Results of these reviews will be fully documented and maintained as official records of the DDA.

c. The DDA will conduct system tests of new WIN applications releases to:

(1) Demonstrate their functionality and stability.

(2) Ensure they meet approved operational and security specifications.

(3) Ensure that security features function correctly under normal operations. (Test objectives do not include efforts to show that the software can withstand penetration attempts.)

d. Testing will be conducted with development copies of applications using test data bases.

e. The volume and variety of test data and the extent of testing will be sufficient to ensure that applications software meets approved security

specifications, and that the software functions in a cohesive, identifiable, reliable, and predictable manner.

f. If operational user files are required for testing, only copies of these files should be used.

g. Upon completion of testing, test results will be fully documented and maintained as part of the DDA's official records.

h. DDAs will certify that results of tests demonstrate that security provisions are adequate and comply with existing WIN security policy.

i. Before release of applications software to WIN multiuser host sites, DDAs will certify to the J6, Joint Staff, that these applications meet approved and documented security specifications.

j. With each new applications software release, DDAs will forward a copy of the applications release test plan (including both operational and security test plans), test materials, and test results to each WIN site to be used by the WIN site to verify correct installation.

3. Development of Site-Unique Applications Software

a. Security specifications for each new site-unique application release will be developed and coordinated with the user, the computer installation manager, and the WASSM or WASSO before approval of the specifications.

b. Security specifications should focus on the functional ability of the system under normal constraints to identify, control, and record individual access to the system and file and to mark ADP products.

c. Design reviews will be conducted by the site to ascertain that the proposed design meets the approved security specifications. The results of the design review should be fully documented and maintained as official records of the site.

d. System tests of each new application release will be conducted to demonstrate that the system meets the approved security specifications and complies with existing security policy. For these tests, it will usually be assumed that the security features of the software can be penetrated under serious and sustained efforts. These tests will ascertain whether the

security features function correctly under normal constraints. Testing should be conducted with development copies of the applications using test data bases. The volume and variety of test data and the extent of testing should be sufficient to ensure that the application will meet the approved security specifications and function in a cohesive, identifiable, predictable, and reliable manner. If operational user files are required for testing during this time, only copies of these files should be used. Upon completion of the system test of each new release, the test results should be fully documented and maintained as part of the official records of the site. Before operational use of the new application release, officials of the site should certify that the application release meets the documented and approved specifications and that results of the test demonstrate that the security provisions are adequate and do not alter existing security policy.

4. COTS Applications Software. This paragraph applies to all COTS software used on WIN multiuser hosts.

a. WIN Standard COTS Applications Software. WIN standard COTS applications software is that software available with WIN standard ADP systems. This software will not be site-modified unless approved by an SDN in accordance with Joint Pub 6-03.11.

b. Site-Unique COTS Applications Software

(1) Before use on a WIN multiuser host, this software will be approved by an SDN in accordance with Joint Pub 6-03.11.

(2) This software will not be site modified and used on a WIN multiuser host unless the modification has been approved by an SDN in accordance with Joint Pub 6-03.11.

5. Public Domain Software and Shareware. Public Domain software and shareware represent a resource that can potentially benefit the WIN community. However, their use presents special risks and can jeopardize operation of the WIN. The risks stem from the fact that shareware is developed in an uncontrolled and undisciplined environment, and is distributed by unsecured means, normally through public bulletin boards. Some of the perils associated with using this type of software include viruses, improperly developed code that does not function as advertised, lack of documentation, and licensing issues. To ensure that the WIN is protected from risks associated with use of public domain software and shareware, their use is prohibited unless the

source code has been approved by the WIN DAA through an SDN in accordance with Joint Pub 6-03.11.

(INTENTIONALLY BLANK)

CHAPTER XII

SYSTEM RESOURCE ACCESS AND CONTROL

1. General. Most reported computer crimes are committed by users with authorized access to the computer system. Discretionary and mandatory access controls and auditing are the last line of defense to detect and prevent unauthorized system and data access. The majority of these controls are based on user identification and authentication.

2. Minimum Requirements for System Access Controls

a. User Identification and Authentication. User identification and authentication is normally accomplished by use of USERIDs and passwords. Other NSA approved methods of authentication may be acceptable, but require SDN approval. All WIN components (multiuser hosts, Remote Datanet 8s, Concentrators, LANs and workstations) using passwords to control user access will use the guidelines of this paragraph.

b. Passwords as User Authenticators. At each WIN multiuser host site, each WIN user will be assigned a USERID. The WASSO or AWASSO is responsible for generating and distributing the initial logon password for each USERID. This password will be classified SECRET. Each password should be expired after the user's first logon so that a new password, unknown to the WASSO or AWASSO, can be obtained. Either a program that follows the CSC-STD-002-85, or a WIN standard password generation and application program will be used by the WASSO for this purpose. The following rules apply to all WIN individual passwords:

(1) Entry of the WIN password on a terminal device will be protected from disclosure to anyone observing the entry process.

(2) The number of password entry attempts will be limited to no more than two successive tries.

(3) Users are responsible for protecting their passwords against loss or disclosure and will be held liable for any improper use of the password.

(4) Logon passwords will not be stored in ADP files by anyone other than the WASSO for issuance to WIN users.

(5) Passwords will be deleted or replaced under any of the following conditions:

(a) Whenever an individual's access is withdrawn for any reason (transfer, discharge, reassignment, temporary or permanent withdrawal of security clearance, release from group USERID team duties, etc.) This will be done immediately if the user's trustworthiness is suspect or, under normal circumstances, within 3 working days from the time the owner's access is terminated, or in the case of a group USERID, if any one user's access is terminated.

(b) Whenever a password or record of a password has been, or is suspected of having been, compromised, immediate notification must be given to the WASSO and WATASO for password replacement and any further appropriate investigative action.

(c) At least semiannually. Local DAAs at their discretion may require that logon passwords be changed more frequently.

(6) For LANs, the LAN Security Manager is responsible for issuing the initial LAN password to users of the LAN.

(7) For workstations with terminal logon password features, the WATASO or workstation administrator is responsible for issuing the initial workstation passwords to users of that WIN workstation.

3. User Identification. Each user will have an individual USERID or be a member of an approved group USERID team.

a. Individual USERIDs. Each individual user will have a unique unclassified USERID.

b. Group USERIDs (General)

(1) Group USERIDs may be approved when use of individual USERIDs would not allow attainment of maximum operational efficiency. They will be assigned by the WIND. Organizations benefitting from use of group USERIDs include command centers, logistic readiness centers, crisis action teams (JCAT), etc. If a group USERID is adopted, a group team chief will be designated in writing.

(2) The downside of using group USERIDs (previously termed "Watch-Team" USERIDs) is that they prevent an automated method of tracking individual activity; i.e., individual accountability is lost. In order to fulfill the DOD Directive 5200.28 requirement for

individual accountability, group USERID team chiefs will maintain a log of group member access. The log will contain the date and time the WIN was accessed, terminal ID, and individual user's name. When group users change places at a terminal, the date and time will be noted in the log. The log will be retained at the discretion of the WASSO.

(3) All team members will possess an interim or final US TOP SECRET clearance. Foreign nationals will not be allowed to be a team member of a group using a group USERID.

(4) The group team chief is responsible for ensuring proper security practices are followed. He or she is responsible for information security associated with the group USERID and will provide a group access list to the WASSO and WATASO, as appropriate. Security vulnerabilities associated with giving the same logon USERID and password to several individuals will be stressed to group team members in a detailed security briefing. Whenever a group member departs the group, and that member knew the group USERID password, the WASSO will be notified. The password will be changed by the team chief under the conditions prescribed by Chapter XII, subparagraph 2b(5) of this publication.

(5) The group USERID concept may be used for formal group network instruction or training. For this purpose, the USERID and logon password will be assigned to the class instructor, who will be responsible for ensuring that proper security practices are followed. The logon password will be changed at the end of each class. Each group USERID or logon password will be associated with a specific instructor. The instructor and the WASSO at the location where training is being conducted will coordinate to ensure compliance with security regulations.

c. Group USERIDs (Single Site). Group USERIDs may be approved by multiuser host DAAs in cases where use of individual USERIDs would reduce operational or mission effectiveness. Group USERIDs approved by the local DAA will not be given WIN access permissions without approval of the WIND.

d. Group USERIDs (Network). If a group USERID requires WIN access permissions, the DAA will approve the group USERID and forward the access request to the WIND for network access approval. The network access request will contain:

(1) Group identity.

(2) Group function.

(3) Name of the group team chief, clearance, and date of clearance.

(4) Identity of the command element responsible for supervising the group.

(5) Telephone number for the group point of contact.

(6) Type of Use. (Daily, peacetime operations exercises or crises.)

(7) Justification. Specify how use of individual USERIDs and logon passwords would adversely affect mission effectiveness.

e. Annual Revalidation of Group USERIDs. Annually, site WSCs will notify the WIND and other WIN site WSCs/WASSOs if continued use of the group USERID is necessary. This notification will include:

(1) Identification of the group.

(2) Group team chief.

(3) The command element responsible for supervising the group.

f. WIN Accessible File of Group USERIDs. The NOC will provide a WIN accessible file of all group USERIDs approved for WIN access. (Joint Pub 6-03.14)

g. Project USERIDs or Accounts. A project USERID or account is a directory or catalog that has subordinate catalogs or directories or files but does not have logon privilege.

(1) Each project USERID or account will have a manager designated as the project’s OPR.

(2) The project account may be used by anyone to whom permissions have been given.

(3) The project manager will protect the project USERID or account password in accordance with subparagraph 2b of this chapter.

(4) The project manager will ensure that project directories are assigned the appropriate security

level and security categories and that files are assigned the proper security classification. The project manager will also ensure that access is not granted to classified files based on general permissions.

h. Revalidation of Individual USERIDs

(1) General. When personnel no longer require WIN access, the passwords through which they had access will be changed. If the associated USERID(s) are no longer needed, they will also be terminated. Multiuser host access revalidation will be performed semiannually by the WSC.

(2) Network. Network access revalidation will be performed semiannually by each multiuser host site.

4. Access to System Resources

a. USERIDs and Accounts

(1) Except as indicated under group USERIDs, logging on to the system will be limited only to individual USERIDs. Project USERIDs will not be used to access the WIN.

(2) OPRs will give specific permissions to individuals and groups for any and all objects to which the individual or group has justified access.

(3) WIN multiuser host's operating system USERIDs or accounts will not be permitted to log on except under specific and controlled conditions. If the site will require terminal access by these system accounts, the account resources may be modified to allow terminal access on a case-by-case basis. The WASSO will approve each such access and ensure that the resources are withdrawn after each access.

b. Site Access

(1) The WSC is responsible for processing WIN access requests in accordance with Joint Pub 6-03.14. The requesting site will verify the user's TOP SECRET clearance in the WIN access request. Approved WIN access requests will be granted WIN access within 5 working days.

(2) When feasible, the user will identify the OPR for each protected file or program to which access is desired. This individual's name and business address or DSN telephone number will be provided to

the requesting WSC before official access is granted. Site procedures will address the required coordination between the WSC, WASSO, and appropriate OPRs.

(3) Access requests will be addressed to each site where permissions are desired stating specifically the justification for needing access at that site. Blanket access requests may be used only by WSCs, WASSOs, or their representatives in performing their system management functions.

c. File and System Permissions. File and data system access permissions will be governed in accordance with Joint Pub 6-03.15.

(1) Positive controls will be used to control access to all classified or special category objects (catalogs, directories, files, etc.) General access will not be given to any classified file or to any file structure containing a classified or special category file. Personnel who depart or no longer need access to a file will have their access permissions deleted as soon as possible by the project or file OPR.

(2) WIN users will be provided with proper procedures for requesting access to WIN files at local and remote sites. The file OPR of the multiuser host where the file resides verifies the need-to-know of the requesting user.

d. Permissions to Functions. Positive controls will be used to control access to all functions that can affect the security or integrity of the WIN. Access of this type will be approved by the WASSO and will be kept to the absolute minimum number of personnel.

5. Audit Requirements

a. General. WIN computers defined in Chapter III will meet the following audit requirements, which are based on DOD 5200.28-STD. Correlation of information on system usage with its associated user requires identification of the user together with his or her activity. If audit analysis detects violations, the site will take corrective action.

b. Minimum Requirements for Accountability. Safeguards will be established to ensure persons having access to the WIN are held accountable for their actions. The audit trail will be capable of providing sufficient detail to reconstruct events in case a compromise has

occurred. To fulfill this requirement, the manual or automated audit trail will document, at a minimum, the following:

(1) Logons, logoffs, timeouts, and lockouts that include time of access and the individual's identity.

(2) Object accesses, creations, deletions, and modifications (successful and unsuccessful).

(3) Activities that attempt to modify, bypass, or negate safeguards or audit data controlled by the system.

(4) Security relevant actions associated with periods processing.

(5) Changing of advisory security levels or categories.

(6) Execution of privileged processes.

(7) Changes in policy rules associated with MLS connections and the flow of data between the WIN and other connected AISs.

c. Audit Sources. Audit records include automated accounting files, console logs, and manual logs that show facility, terminal, and information access. Because automated accounting files are processor-specific and may include more information than minimally required by subparagraph 5b above, the WASSO will determine which audit records constitute the mandatory audit trail. Assistance may be available in the form of an STP that identifies suggested records to be reviewed and maintained. Audit sources will be determined by the WASSO.

d. Audit Trail. The audit trail provides a record of system activity. The WASSO will identify and recommend appropriate actions on security related events in the audit trail. System surveillance will be under the control of the WASSO, who interacts with the computer center operator, system maintenance programmers, hardware maintenance personnel, and system users. Audit trails will be reviewed at least weekly (or less at the discretion of the WASSO) with follow-up action taken on all discrepancies. Suspected security incidents that occur during network processing will be reported to the local site WASSO for action. The NOC, a support element of the WASO, will be notified of any serious actions

planned or taken as a result of the incident investigation.

e. Review Requirement

(1) Machine-Specific. Audit data defined in the machine-specific STP will be reviewed periodically. Incidents will be reported as required in Chapter I.

(2) Network. Network audit reports give detailed information for each process executed on the network and provide summary accounting information on each USERID, account, or process. These reports will be available for review by the WASSO for each period of WIN operations. The WASSO will be informed of any activities that are suspect. The WASO will be informed by the site WASSO or NOC of security incidents that are related to network operations. This cooperative effort among the sites will be coordinated through the offices of the NOC. The individual site's efforts are monitored by the WASSO.

f. Disposition of Mandatory Audit Records. The site records, which comprise the audit trail, will be retained at the discretion of the WASSO. The multiuser host DAA may authorize conversion of the audit trail to hard copy or computer output microfilm. Thereafter, the file will be disposed of in accordance with DOD Regulation 5200.1-R and applicable site records management procedures.

6. System Profile and File Structure Management. The WASSO should analyze the system master profile and file structure daily for discrepancies. At a minimum, the analysis will check for the following items:

a. Unauthorized new users or accounts.

b. Increased user resources.

c. System accounts with logon resources.

d. Unauthorized permissions for system privileges.

e. Resources used that are greater than allowed limits.

7. Privileged States and Functions

a. Jobs, processes, or users that require privileged states or functions will be authorized only by the multiuser host DAA or a designated representative. A listing of those jobs, processes, or users will be

maintained in the site for the operators to verify approval prior to granting privity.

b. Standard or Service-unique WIN application systems will not be developed with a privileged-state requirement unless prior approval of the network DAA has been received.

8. Shutdown and Restart

a. Scheduled shutdown and restart during a processing period will follow the procedures described in the site operations manual. An audit record will be written to the accounting file uniquely identifying the reason for system shutdown. A system dump need not be taken unless requested by the WASSO or the site system analysts. The system can be restarted with site-dependent warm boot procedures.

b. A system dump will be taken following any system crash of unknown cause. An audit record describing the system condition will be entered in the accounting file.

c. Emergency shutdown will include the necessary site dependent power-off procedures. Backup copies of user files will be available for restart.

d. Shutdown procedures at the end of a period are site dependent. The removable media will be removed, hardware reconfigured if necessary, output removed, accounting tape and startup deck returned to the library, and peripheral subsystems that are not required will be turned off.

9. Terminal or Workstation Time Out. WIN multiuser host operating system software parameters will be set so that all multiuser host-connected terminals and workstations time out after 10 minutes if they have processed no input or output transactions to or from the WIN multiuser host. The purpose of this requirement is to ensure that terminals inadvertently left unattended, but turned on, are exposed to minimum risk of unauthorized use. This 10-minute requirement can be adjusted by the multiuser host DAA when exercises, crises, or other unusual circumstances are involved.

10. Split Systems and Periods Processing

a. WIN multiuser hosts can operate in a periods-processing or a split-system mode, if desired. Before categories requiring special controls (e.g., SCI, SIOP-ESI, COSMIC, NATO, or CNWDI) are introduced at a WIN

site, that system will be physically disconnected from the WIN and periods processing will be used.

b. Between periods-processing sessions, memory will be cleared using DISA-evaluated and WIN DAA-approved software. The clearing will be verified. The system packs and removable media, classified at the level appropriate for the period, will be used at system startup. The peripheral subsystems will be initialized according to site procedures.

CHAPTER XIII

HARDWARE SECURITY

1. Hardware Security Features. Hardware resident architectural features are important elements in COMPUSEC. Security requirements will be included as procurement selection factors. Hardware to be used in the WIN will be approved through the SDN process, in accordance with Joint Pub 6-03.11, and will have configuration management controls to protect it against unauthorized alteration.

2. Hardware Declassification. Hardware will be declassified in accordance with Chapter XVI of this publication at the end of each day's processing unless it is located in a storage area approved for TOP SECRET open storage. If the hardware becomes inoperable, it will be protected at the TOP SECRET level until destroyed and a destruction certificate is initiated.

3. Nonremovable Magnetic Media. Nonremovable magnetic media have special security requirements and problems that affect their use.

a. End of Day. Nonremovable magnetic media will be declassified at the end of operations each day or kept in an area approved for open storage of TOP SECRET information.

b. Maintenance. Nonremovable magnetic media will be declassified prior to turn-in for maintenance. Clearing by overwriting with DISA-approved overwrite software is an acceptable means of declassification for magnetic media where the destination is a Government or contract maintenance facility with eventual return to use on the WIN. If the nonremovable magnetic media is inoperable, the overwrite will fail. In this case, the nonremovable media would have to be removed before turn-in, potentially causing maintenance contractual problems.

c. Decommissioning. Hardware that is to be decommissioned and no longer operated on the WIN will have its nonremovable magnetic media declassified. Magnetic media to be decommissioned will be purged to achieve declassification. Clearing by using overwrite software together with a low-level format of the media may be used for purging if approved by the WASSO. WASSOs should consider the media's history as a factor in making the decision on how to declassify. Media known to have stored large quantities of classified data should be degaussed, whereas media known to have had minimal exposure to classified data may be declassified by overwriting.

4. Test and Diagnostic Equipment. Security considerations for using T&DE are discussed in Chapter XVI, paragraph 9.

5. Spare Parts. Memory component spare parts (such as memory boards) for WIN hardware will be protected at the TOP SECRET level when they are on-site and identified as WIN hardware spare parts. Vendors will be instructed not to specifically identify WIN hardware spare parts as such when the spare parts are off-site in the vendor's possession.

6. Foreign Vendor Hardware and Firmware

a. Hardware. WIN hardware end items, such as CPUs, stand-alone disk drives, and workstations will not be procured from foreign vendors even though manufactured in CONUS, unless previously approved by the Joint Staff, J-6.

b. Firmware. ROMs, PROMs, and other varieties of precoded memory chips identified for use on the WIN will not be procured from a foreign vendor without Joint Staff J-6 approval.

7. Hardware Modification. There will be no modifications to WIN hardware without prior notification of the WASSO. Generally, there will be no modifications to the hardware unless they are:

a. Part of a maintenance contract.

b. Site unique and preapproved by an SDN in accordance with Joint Pub 6-03.11.

8. Distribution of WIN Hardware

a. Hostile attacks may occur on WIN multiuser host computers when they are in use. But, it is also possible for them to be attacked before they are installed. Hardware intended for use in the WIN will be protected to minimize hostile attacks. Precautions will be taken to ensure that all hardware, firmware, and software products delivered from a contractor or another site are operating under a correct implementation of the system's security policy. This includes assurance that:

(1) The product evaluated is the one the manufacturer built.

(2) The product built is the one that is sent.

(3) The product sent is the one that is received.

(4) The product received is the one that is installed.

b. For distribution of multiuser host hardware, peripherals, or workstations, the sender will use either registered mail or courier in accordance with NCSC-TG-008. In either case, the products delivered will be marked for attention of the WASSO. The WASSO or WATASO will inspect the incoming shipment to validate that no tampering has occurred.

c. If the WASSO’s inspection of the received hardware reveals evidence of tampering, it will be assumed the hardware received has been tampered with or bugged. A TSCM inspection of this hardware will be performed before it is installed. A security incident report will be initiated in accordance with Chapter I, paragraph 8, of this publication.

(INTENTIONALLY BLANK)

CHAPTER XIV

EMANATIONS SECURITY

1. Emanations Security Policy. All electronic information processing devices radiate electromagnetic energy that can be received and exploited using proper equipment. To guard the WIN against this type of exploitation, the following policy is set forth.

a. WIN users will comply with the measures to control compromising emanations provided under DOD Directive C5200.19, "Control of Compromising Emanations."

b. The risk of using equipment that produces compromising emanations will be different at each WIN site. The countermeasures to be implemented for WIN sites will be determined in accordance with NTISSI 7000. In all instances, a security and cost analysis of the possible countermeasures should be made before making a final decision. On-site vulnerability analysis, tests, and inspection or other appropriate verification procedures will be used to demonstrate TEMPEST countermeasures acceptability. After evaluating the risk and considering the cost of effective counter-measures, the WIN multiuser host DAA may elect to accept a higher risk by not implementing countermeasures to the level determined in accordance with NTISSI 7000. If this decision is made, it will be documented, with justification, in the site Risk Analysis.

2. TEMPEST. The primary documents that will be used to determine the degree of TEMPEST protection against emanations are NTISSP 300, "National Policy on Control of Compromising Emanation" and NTISSI 7000, "TEMPEST Countermeasures for Facilities" or implementing Service regulations. Implementation of these policies is mandatory. Furthermore:

a. Where use of equipment meeting national standards contained in the National TEMPEST Standard, NTISSAM TEMPEST/1-91, is indicated, products on the ETPL should be used.

b. Devices that have no known TEMPEST profile will be tested before being installed on site to determine the CS required, minimum essential countermeasures required, or possible equipment modification. If the equipment model has not been previously tested (i.e., has no known TEMPEST profile), it may be tested by sending the equipment to the appropriate Service or Defense agency or, preferably, by having an on-site survey.

3. TEMPEST Maintenance Considerations. Device emanation characteristics are sensitive to the manner and quality of repair and to changes or modifications accomplished. Maintenance and service personnel will be made aware of this sensitivity. When repairs or changes are made to meet prescribed emanation requirements, every effort should be made to use exact replacement components or components known to possess equivalent or superior TEMPEST characteristics. If this cannot be done, a new TEMPEST survey will be accomplished.

4. COMSEC and EMSEC OPR. Each Service has an office that is the designated OPR for COMSEC and EMSEC matters. Questions concerning the scheduling of TEMPEST tests, applicability of NACSIM 5203 RED/BLACK criteria, requirements for filtered power, options concerning the installation of telephone instruments and lines, shielding, and other such problems may be forwarded through the appropriate channels to the designated Service or Defense agency COMSEC/EMSEC OPR.

CHAPTER XV

COMMUNICATIONS SECURITY

1. COMSEC Policy. Transmission and communications lines and links that provide secure data communications among WIN devices or among WIN sites will be secured in a manner appropriate for TOP SECRET material, transmitted through such lines or links under the provisions of DOD Directives C-5200.5 and 5200.1.

2. Data Communications Links. Communication links among WIN sites will meet the security requirements for the transmission of TOP SECRET data as well as all restrictive categories of material processed by attached devices.

a. Security Control and Protection. To ensure the required security control and protection, the WASSO will determine the restrictive categories that may be transmitted on each communications circuit.

b. Red Side Circuit. For WIN devices (e.g., terminals, workstations.) connected to other devices (e.g., multiuser hosts, LAN interface units) over dedicated communications lines, the red-side circuit will be capable of being disconnected (e.g., at a patch panel) at each location. The connection will be labeled to identify the specific device, level of information access authorized, and restrictive categories of information that are authorized for access from the specific device.

3. Dial-Up Devices. The initial installation of dial-up devices at a WIN multiuser host will be specifically accredited by the WIN DAA prior to operation. Use of dial-up devices for encrypted data transmission requires the dial-up devices to be physically located in the same TOP SECRET control zone as the system component to which it is attached and be afforded the same protection as other WIN components. Connecting secure dial-up devices to a WIN multiuser host requires:

a. Thorough evaluation by the multiuser host DAA of the risks involved.

b. All communications connections will be in compliance with NACSIM 5203, "Guidelines for Facility Design and Red/Black Installation."

c. When the device, crypto, and associated modem are connected, physical security will be provided in accordance with requirements established in Chapter VIII of this publication.

d. Supplementary control will be established to audit the identity of the device making the connection. Examples of such controls include the use of:

(1) Dial-back modems.

(2) Approved authenticator systems.

(3) A machine-readable, unique-device identifier stored within the device or its associated communications equipment.

e. A list of approved dial-up devices will be maintained at the hosting WIN site and will contain:

(1) The device identifier.

(2) The level of information access authorized.

(3) All restrictive categories of information that are authorized for access from the specific device.

f. All terminal access attempts will be audited.

g. Telephone numbers and devices with call forwarding capability will not be used.

4. STU-III. The Type 1 STU-III is a dual-purpose telephone capable of transmitting classified voice and data over the public telephone network. Because it represents a cost-effective alternative to installing expensive crypto equipment and protected wiring distribution systems into remote facilities where WIN terminals may be required, the Type 1 STU-III is authorized for data communications between remote terminals and WIN multiuser hosts. To ensure proper use of the STU-III when employed with the WIN, users will comply with the operational security doctrine of NTISSI No. 3013. In addition, the following policy is set forth.

a. Use Within a TOP SECRET Control Zone. The normal location for WIN remote terminals is in an area complying with the physical security requirements of Chapter VIII of this publication. Use of the Type 1 STU-III under these conditions is authorized and will comply with the following conditions:

(1) The Type 1 STU-III will be equipped with the SACS. This capability permits users to operate the device in either an attended or unattended mode (with restrictions listed below) by providing automatic and unattended authentication for data connections.

(2) Operating in the Attended Mode. Operating the STU-III data port in the attended mode is acceptable under the following conditions:

(a) The STU-III will be physically located in the same TOP SECRET control zone as the WIN terminal/workstation/multiuser host to which it is attached. Other security precautions afforded the WIN terminal/workstation/multiuser host also will be provided.

(b) The STU-III will be programmed to accept only TOP SECRET connections. This capability causes the telephone to reject connections with other STU-IIIs that are not also programmed as TOP SECRET.

(c) The STU-III will not be allowed to be connected to another STU-III for more than 24 hours in a single session. After 24 hours, the session will be terminated, and a new session can be initiated, if necessary.

(3) Operating in the Unattended Mode. Operating the STU-III data port in the unattended mode is permitted by meeting the above conditions, combined with the use of DAO codes that specify department, agencies, or organizations. This procedure enables the user to further restrict access by specifying that the STU-III accept calls only from specific DAO codes.

b. Use Outside a TOP SECRET Protected Control Zone. When used outside a TOP SECRET control zone, a securable container such as the Secure Desk (KWS-5203) that meets the physical security requirements of Chapter VIII of this publication will be used. Use of the STU-III in these securable containers is authorized subject to the following conditions:

(1) The conditions of subparagraph 4a above are observed, except that the STU-III will not be operated in the unattended mode.

(2) The securable container has been authorized for use by the multiuser host DAA.

(3) Operation of the WIN terminal in the securable container conforms to the conditions specified in Chapter VIII of this publication.

(4) While in use, the STU-III will be located inside the securable container. This will ensure

that no communication lines between the WIN terminal and the STU-III are exposed and subject to a threat attack.

c. Use of the STU-III on the DSN. Use of STU-IIIs on the DSN will comply with CJCS MOP 8. CJCS MOP 8 states that the DSN will not normally be used for data transmission, because this function is primarily the responsibility of DDN. However, CJCS MOP 8 does state that "Data processing equipment may use DSN voice circuits only when DDN and other transmission media, either commercial or government owned, do not exist or are required for emergencies or reasons of national security and are authorized in subparagraph 1a(6)(b)2 of MOP 8. Use of the DSN switched voice (dial-up) circuits to transmit digital data will not be detrimental to voice users." This subparagraph specifies approval authority, coordination requirements to determine network impact, and the requirement for annual revalidation. The approval authority for OCONUS data transmission through DSN voice dial-up circuits is the CINC. The CONUS approval authority is the CINC, Chief of the Service, or Director of the Defense agency concerned.

d. Portable Terminals. STU-IIIs may be used to provide communications for portable WWMCCS workstations or terminals. The terminals will be protected in accordance with the policy of this publication.

5. AUTODIN Interface. AUTODIN is a telecommunications network complying with all COMSEC requirements for the transmission of classified information up to and including TOP SECRET. WIN connections to AUTODIN will ensure that the security protection of AUTODIN is not diminished. Connection to AUTODIN requires that the AUTODIN connection be accredited as described in Chapter V.

CHAPTER XVI

INFORMATION SECURITY

1. General. The WIN operates in a TOP SECRET system-high mode. As such, all features of the system, including output products and storage media, will be classified TOP SECRET until determined otherwise.

2. Accountability of Output Products

a. Output Products. Output products include, but are not limited to, such items as printed listings, microfilm, microfiche, and CRT displays.

b. Formal Accountability. Formal accountability of WIN output products as TOP SECRET documents (DOD Regulation 5200.1-R) is not required unless the user producing the output verifies actual TOP SECRET data is present. The one exception to this is a computer dump, which will be handled and marked as "TOP SECRET Working Papers" until reviewed by a qualified analyst for the actual classification of the content. Organizations with on-line printers, whether in the central computer facility or in a terminal area (remote line printer), will require that users and customers sign for output. A log identifying the output product by unique identifier, date, and the user or customer may be used for this purpose. (The log should be retained for one year.) Users and customers will protect output products as if they were TOP SECRET until they have been reviewed and the actual classification confirmed. Formal accountability of TOP SECRET output products is the user’s or customer’s responsibility.

3. Marking Output Products. WIN output products will be marked with the proper classification for the data present. Normally, unclassified material will not be marked or stamped "UNCLASSIFIED" unless it is essential to convey to a recipient of such material that it has been examined to determine its classification. When feasible, the products should be marked by the ADP system that generated it and should include the originator, a unique identifier, classification authority, and downgrade instructions.

a. Printed Paper Products. Printed paper products will be marked with the user’s intended security classification on the top and bottom of each page. Unless technically or operationally infeasible, the first page of the product will be marked with the safeguard statement shown in Figure 16-1, as well as declassification instructions of DOD 5200.1-R. Each page of a multipage product will be sequentially

numbered. The user is responsible for ensuring the continuity of page numbering after receiving the product.

*** SAFEGUARD ***

HANDLE AS TOP SECRET INFORMATION UNTIL SIGNED BY AN 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 UNUSUAL OR UNREQUESTED OUTPUT DISCREPANCIES IMMEDIATELY TO: (WASSO, ROOM NUMBER, PHONE NUMBER). I HAVE REVIEWED THIS DOCUMENT AND, BASED ON THE CONTENT, FOUND IT SHOULD BE

CLASSIFIED:

SIGNATURE: DATE:

Figure 16-1. Safeguard Statement

b. Microfilm and Microfiche. These products will be conspicuously marked (i.e., eye readable) with the highest security classification of the data contained therein, date of creation, and unique identifier. Information identifying product originator, as well as downgrading and declassification instructions or exemptions will be either displayed in the first image or printed on the special container or envelope provided for storage. Each image will have a security classification marking that is clearly visible on the top and bottom when the image is magnified.

c. CRT Displays. Operating system software should provide classification screen markings for CRT report products. If this does not occur, the printed listing of a CRT screen produced on a screen printer will have classification markings added manually by the user except when the printed listing is unclassified. In addition, the CRT should be physically marked (i.e., place a sticker or other physical label on the CRT case) TOP SECRET.

4. Accountability of ADP Storage Media

a. Media. ADP storage media include items such as magnetic tapes, disks, diskettes, disk packs, and removable hard disk cartridges.

b. TOP SECRET Accountability Requirements. Removable ADP storage media used on hardware attached to the WIN

does not require formal TOP SECRET accountability in accordance with DOD 5200.1-R unless it leaves the boundaries or confines of the WIN TOP SECRET central computer facility or terminal areas and has not been downgraded to a lower classification.

NOTE: The terms "boundaries" or "confines" of an approved ADP system refer to the outer perimeters of the continuously protected areas housing the central computer facility and connected remote terminals as prescribed in DOD Manual 5200.28-M.

5. Marking ADP Storage Media

a. Marking. Removable ADP storage media used on hardware attached to the WIN will be externally marked TOP SECRET until declassified or downgraded. This marking will be written and color-coded orange. The use of color-coded media or media labels is required. Additionally, the media will be externally marked:

(1) With special access restrictions, if applicable.

NOTE: This should not be confused with special access programs prohibited by Chapter I of this publication.

(2) With a permanently assigned identification or control number to aid in inventory control.

(3) If the media is a nonremovable disk drive, the cabinet housing the disk will be conspicuously marked TOP SECRET.

b. Exceptions. Exceptions to the marking requirements of subparagraph 5a above are:

(1) UNCLASSIFIED, CONFIDENTIAL, or SECRET removable magnetic media used for uploading data to the WIN that have a "Write Protect" mechanism installed each time the floppy disk is used on a WIN workstation.

(2) UNCLASSIFIED, CONFIDENTIAL, or SECRET reel-to-reel tapes used for uploading data to the WIN that do not have "Write Enable Rings" installed.

(3) UNCLASSIFIED, CONFIDENTIAL, or SECRET cassettes or streaming tapes used for uploading data to the WIN that have a "Write Protect" mechanism in place.

6. Clearing, Declassification, and Downgrading of WIN Magnetic Storage Media

a. General. The terms "clearing" and "declassification" are functional definitions referring to the method and result of removal of classified data from magnetic storage media. The distinction between the two procedures lies in the purpose for which each is performed, as well as the techniques and procedures employed. Downgrading of magnetic media refers to the lowering of its classification after an administrative review has validated the actual classification of the data residing on the media to be the lower classification. The terms "clearing" and "declassification" are defined as follows:

(1) Clearing of Magnetic Media. Clearing of magnetic media is the removal or erasure of classified data recorded on that media in such a way that there is assurance, proportional to the sensitivity of the data, that the data may not be reconstructed using normal system capabilities; i.e., through the keyboard. (This includes use of advanced diagnostic utilities.) The procedure may be accomplished by overwriting the media with software that writes to every addressable location (including bad sectors) on the media with a complement pair (e.g., a binary "one" and then a binary "zero," and a random pattern). Clearing is normally used when magnetic media will be reused for another purpose within the WIN, will continue to be safeguarded, and will remain either within the same secure WIN computer facility or another WIN computer facility. The media may remain connected to the WIN during the procedure.

(2) Purging. Purging is the removal or erasure of classified data recorded on that media in such a way that there is assurance, proportional to the sensitivity of the data, that th
e data may not be
reconstructed using an open-ended laboratory techniques. Purging may be accomplished by overwriting, degaussing, or destruction. If overwriting is selected, the software used must be SDN approved and capable of overwriting all sectors of the disk as described above under "Clearing." The media must be removed from the WIN prior to the procedure.

(3) Declassification of Magnetic Media. Declassification of magnetic media is the removal or erasure of classified data recorded on that media by clearing or purging followed by the administrative action of removing the classification. An administrative review is required to provide assurance that the declassification procedure is

certified to perform its function and that it was used properly, or that the destruction procedure was carried out correctly. The declassification is complete only after submission to the appropriate authority (e.g., WASSO) a decision memorandum stating the procedure is complete and verified. Declassification may render the media unusable.

(4) Downgrading of Magnetic Media. Downgrading magnetic media used in the WIN is defined as the lowering of the classification of the media from TOP SECRET to the level of the actual classification of the data contained therein. This is not to be confused with the definition of information downgrading contained in DOD Regulation 5200.1-R, which refers to lowering of the classification level of data. If the information contained on the media can be determined to be classified at less than TOP SECRET, then the media may be downgraded to that level. Downgrading WIN magnetic media does not normally involve a downgrading of data.

b. Policy

(1) Clearing of Magnetic Media. Clearing of magnetic media will be used when data stored on the media is no longer required by the data owner, but the media will continue to be used for the WIN. Clearing of magnetic media is the responsibility of the data owner and will be executed by computer operations personnel upon receipt of an official request by the data owner. Clearing will be accomplished with overwrite software that has been approved by the WASO.

(2) Declassification of Magnetic Media. To provide the highest degree of assurance that classified information has been removed from the media, purging (validated overwriting, degaussing, or destruction) must be used.

(a) Declassification will be used when the media is to be decommissioned or released into a less than TOP SECRET or nongovernment-controlled environment.

(b) Declassification of WIN magnetic storage media is a security auditable event. Accordingly, upon completion of the declassification procedure, a written Declassification Audit Report will be submitted to the WASSO or WASSM. It will be retained for a period of 1 year. The report will include:

1. Identification, last location used on the WIN, and destination of the media that was declassified.

2. Identification of the person who performed the declassification procedure.

3. Date, time, and location where the declassification procedure was performed.

4. Identification of the declassification procedure used and a description of the validation process.

(3) Downgrading of Magnetic Media. Frequently, there exists a need to transfer WIN data to other AISs classified at levels lower than TOP SECRET. To effect transfer and downgrade of this data, the following actions will be accomplished:

(a) The WIN data to be transferred will be identified and determined to be actually classified at or below the classification level of the AIS to which it is targeted.

(b) This data will be copied to new unclassified or declassified media.

(c) Upon completion of the copy, the new media will be reviewed to ensure that only the data intended was copied to the new media. To set the classification level of the new media, two actions are necessary:

1. A record count or file size of the files copied to the new media will be compared to that of the old media to ensure no aberrations occurred during the copy process.

2. A random sample composed of not less than 10 percent of all media storage locations (including those that are beyond the end-of-file marks) will be output to hardcopy or CRT and reviewed by someone competent to determine the actual classification of the data. The media can then be marked with the actual classification of the data therein. The DISA will be responsible for developing software to meet this output requirement for media used on standard WIN hardware.

(4) Approved Procedures. Clearing and declassification procedures contained in "A Guide to Understanding Data Remanance in Automated Information Systems (NCSC-TG-025), Version 2," are acceptable methods for use on WIN equipment.

c. DISA Responsibilities. DISA will provide each WIN site with SDN-approved overwrite and output software and will serve as the configuration manager for that software.

d. WASSO/WASSM Responsibilities. WASSOs or WASSMs will ensure that SDN-approved software, NSA approved hardware (degaussers), and procedures are available for media clearing and declassification.

7. Declassification of Nonmagnetic Permanent Storage Media. Destruction is the only approved method of declassifying nonmagnetic storage media. An example is the WORM optical drive. As other nonmagnetic permanent storage media become available, requests to declassify these media by means other than destruction will be submitted to the WASO for approval.

8. Declassification of Semiconductor Memory

a. Volatile Semiconductor Memory. Semiconductor memory will be declassified by removing all power (external and battery) for a period not less than 5 minutes.

b. Nonvolatile Semiconductor Memory. Nonvolatile semiconductor memory devices such as ROM, EPROM, EEPROM, etc., will be declassified either by overwrite or destruction, as applicable.

9. Test and Diagnostic Equipment. WIN hardware and software maintenance personnel (both Government and contractors) sometimes use T&DE to perform their maintenance function. If this T&DE is connected to WIN equipment, there is a risk that classified WIN data could be transferred to the T&DE. Therefore, T&DE and its removable media, such as floppy diskettes, will be considered to contain TOP SECRET data and will be declassified or downgraded to UNCLASSIFIED before being removed from the WIN site. For all T&DE, contractors will provide the site WASSO with written verification from the contractor’s company that the T&DE can be declassified or downgraded and the procedure for declassification; e.g., removal of power. The site WASSO will review the procedure and ensure that only T&DE so verified is used on WIN equipment. Unless the T&DE is to be continuously connected to the WIN, TEMPEST requirements do not apply.

(INTENTIONALLY BLANK)

CHAPTER XVII

WORKSTATION SECURITY

1. General. Workstations differ sufficiently from multiuser hosts in function, operation, resource allocation, and access control to warrant special consideration in this publication. Because they are intelligent workstations capable of permanent storage, file transfer to and from WIN multiuser hosts, and connectivity to other workstations, they pose added security risks as compared to dumb terminals. Therefore, the policy set forth in this chapter is designed to address these risks and provide additional guidance to ensure workstations are used securely while attached to the WIN.

2. Approval to Connect a Workstation. Approval to connect a workstation to the WIN is obtained in the same manner as other devices; i.e., through the SDN process. In addition, the requirements of Chapter V of this publication must be met.

3. Resource Access and Control

a. Workstation Safeguards. Classified WIN data files may reside on WIN microcomputer workstations. Some of this data may have restricted access; i.e., some users may not have a need to know for the data on the workstation. To ensure that need-to-know barriers are not crossed by users on a given workstation, one of the following safeguards will be implemented.

(1) The workstation will be operated, at a minimum, with the functionality of a Computer Security Evaluation Class of C2 (See DOD 5200.28-STD).

(2) At a minimum, need-to-know separation of data will be maintained. (This safeguard will be implemented only if the functionality of a C2 class is not achievable.)

b. Workstation-to-Workstation Connectivity. Workstation-to-workstation connectivity is authorized, provided:

(1) Workstations maintain the same level of identification, authentication, access control, and audit as the WIN multiuser host.

(2) Each workstation user and administrator possess a unique USERID and a unique password corresponding to it.

(3) Workstation administrators ensure that users do not inadvertently gain unauthorized privilege through remote access to another workstation.

4. Physical Security

a. The provisions of Chapter VIII, especially paragraphs 3 and 5, apply to WIN terminal areas and, thus, apply also to WIN workstations. In addition, terminal area WIN hardware will be labeled as follows:

"THIS EQUIPMENT IS FOR USE ON THE TOP SECRET WWMCCS INTERCOMPUTER NETWORK. IT WILL BE PROTECTED AS TOP SECRET AT ALL TIMES. IT WILL NOT BE MOVED OUT OF THE TOP SECRET WIN AREA OR CONNECTED TO NON-WIN SYSTEMS WITHOUT PRIOR APPROVAL OF THE WATASO. IT WILL NOT BE RECONNECTED TO THE WIN WITHOUT PRIOR APPROVAL OF THE WASSO."

b. Workstation Lockout. If facility maintenance personnel, such as carpenters or painters, are going to be in the terminal area for an extended period of time, workstations should be locked out at the multiuser host and removable media stored in appropriate containers. To prevent bugging of the hardware or terminal area, escorts are required for facility maintenance personnel, even when workstations are locked out.

5. Privately Owned Hardware and Software. Privately owned hardware and software; i.e., not procured and owned by the US Government, will not be used on the WIN unless specifically approved by an SDN.

6. Periods Processing. If workstations are required to operate in a mode other than TOP SECRET system-high (stand alone or connected to another network), the following minimum requirements will be met:

NOTE: These restrictions are not intended to bar the use of COTS software to produce UNCLASSIFIED non-WIN-related documents, briefing charts, etc., by WIN users. An example of when periods processing would be required is when non-WIN users must use the computer for non-WIN purposes.

a. The workstation will be physically disconnected from the WIN.

b. Workstation magnetic media will be removed.

NOTE: If the workstation has nonremovable magnetic media, it will be downgraded to the appropriate

classification level or declassified by overwriting.

c. Workstation internal memory will be cleared by powering off the workstation and leaving it off for a minimum of 5 minutes.

d. The workstation will continue to be physically protected at a TOP SECRET level. If the workstation is to be used outside the WIN site, Chapter VIII, paragraph 5, "Protection of WIN Hardware," applies.

e. Separate operating system software and utilities will be maintained for processing information in modes other than TOP SECRET system-high.

f. Written periods processing procedures will be maintained in each WIN terminal area. These procedures will be included in WIN security training for the terminal area users.

7. Security Administration. Multiuser intelligent workstations will have a security administrator assigned to perform security administration for the workstations. These administrative duties include:

a. Assignment and management of workstation individual and group (if applicable) USERIDs.

b. Assignment and management of workstation passwords.

c. Collection, review, reduction, and archiving of workstation audit data.

d. Definition and maintenance of user access profiles.

e. Creation and maintenance of system directories and files.

f. Management of backups and recoveries.

g. Installation of new software and device drivers.

h. Other system and security administrative duties, as required.

8. Audit. Audit on the workstation will be used to detect and deter penetration and to reveal usage that identifies misuse. Accordingly, users and Security Administrator’s actions will be open to scrutiny by means of audit. The audit’s purpose relates to the requirement for individual accountability as specified in the DOD 5200.28-STD (Orange Book) Accountability Control Objective, which states:

"Systems that are used to process or handle classified or other sensitive information must assure individual accountability whenever either a mandatory or discretionary security policy is invoked. Furthermore, to assure accountability the capability must exist for an authorized and competent agent to access and evaluate accountability information by a secure means, within a reasonable amount of time and without undue difficulty."

a. Minimum Workstation Audit Requirements

(1) Audit data will be selectively acquired based on auditing needs determined by the workstation Security Administrator. At a minimum, the following events will be audited:

(a) Startup and shutdown.

(b) Logon and logoff.

(c) Object create, modify, or delete.

(2) In any case, there must be sufficient granularity in the audit data to support tracing the auditable events to a specific individual who has taken the actions or on whose behalf the actions were taken.

b. Required Audit Capabilities. Audit mechanisms on audit capable WIN multiuser intelligent workstations will be capable of meeting the functional audit requirements specified by DOD 5200.28-STD for the C2 criteria class. Specifically, the audit mechanism will be capable of selectively auditing the following events:

(1) Use of identification and authentication mechanisms.

(2) Introduction of objects into a user’s address space.

(3) Deletions of objects from a user’s address space.

(4) Actions taken by computer operators and system administrators or system security administrators.

(5) All security-relevant events. (See Glossary for definition of a security-relevant event.)

(6) Production of printed output.

c. Auditable Information. The audit mechanism will be capable of recording the following audit information:

(1) Date and time of the event.

(2) Unique identifier on whose behalf the subject generating the event was operating.

(3) Type of event.

(4) Success or failure of the event.

(5) Origin of the request (e.g., workstation ID) for identification and authentication events.

(6) Name of the object introduced, accessed, or deleted from a user's address space.

(7) Description of modifications made by the system administrator to the user or system security databases.

d. Security of the Audit Mechanism. The audit mechanism will be secure from user or unauthorized manipulation.

(INTENTIONALLY BLANK)

CHAPTER XVIII

WIN SITE CONTINGENCY PLANNING

1. General

   a. WIN site contingency operations plans affect system reliability and system stability, which are two of the minimum security requirements of DOD Directive 5200.28. Therefore, plans to provide for continuity of operations under conditions ranging from total WIN site destruction to degradation or loss of one or more requisite automation resources will be formulated.

   b. In accordance with Joint Pub 6-03.14, WIN sites will submit copies of site contingency plans to the WIND.

   c. Classification guidance will be in accordance with Appendix B of this publication.

   d. FIPS Pub 87, "Guidelines for ADP Contingency Planning" is recommended for use in the preparation of these requirements.

2. WASSO Involvement. Because planning required for continuity of operations is critical, site AIS managers are responsible for formulation and initial testing of site contingency plans. The site AIS manager will also periodically conduct a review and test of these plans. Although responsibility for site contingency plans is a site AIS manager’s function and crosses all areas of AIS operations and INFOSEC, the assigned WASSO has a vested interest. The WASSO’s security technical contributions can be invaluable to the overall viability of the plans. Site DAAs, therefore, are encouraged to seek their WASSO’s involvement at an early date.

(INTENTIONALLY BLANK)

CHAPTER XIX

MALICIOUS SOFTWARE

1. General. "Malicious software" is a class of computer code that has been written and inserted into computer software for the purpose of causing damage (directly or indirectly) to computer systems or networks.

2. Malicious Software Sources. Software produced or duplicated on a microcomputer that has been infected is the most likely source of malicious software. The most common classes of malicious software are those that are inserted into published, useful, and popular products for which there is a normal high market demand. The author of malicious software typically inserts a virus, worm, or trojan horse (generally a small object code fragment) into an executable copy of a software application or operating system product which, when executed on a microcomputer, produces undesirable effects. Even though use of software on the WIN is regulated through the SDN process, malicious software can be introduced into the WIN through approved COTS software packages, either at the time of manufacture or at the time of duplication for distribution.

3. Effects of Malicious Software on the WIN. Introduction of infected software into a WIN microcomputer workstation may infect that workstation and expose others if the infected programs are transferred across the network. Users of infected microcomputers are normally unaware of the condition. The damage that can result is real. Nevertheless, users who violate the policy of this publication and introduce malicious software into a WIN workstation are exposing the WIN to unnecessary risks and will be prosecuted in accordance with applicable laws and regulations.

4. Policy. Positive actions will be taken by management, technical support personnel, and users to protect the WIN from malicious software. In particular, the following actions are required.

a. Education. Personnel associated with the WIN will familiarize themselves with materials that discuss the nature, variety, mechanisms, and effects of malicious software. It will be their responsibility to understand how malicious software can be introduced into a computer or network, how it works, vulnerabilities it exploits, protection strategies, control measures, and disaster recovery.

b. Training. Personnel associated with the WIN will be introduced to malicious software as part of their introductory training. Thereafter, on an annual basis,

additional training will be received, particularly on the latest threat developments.

c. Virus Prevention Program. In addition to the normal security program in place, site management will procure COTS antiviral software that is designed to detect and, in some cases, correct malicious software. WIN multiuser host DAAs will institute procedures to ensure that a scan is made of all WIN microcomputers for malicious software at the following times:

(1) PRIOR to their first connection to the WIN.

(2) On at least a monthly basis.

(3) When a new software product or product upgrade is installed.

(4) When any new diskette is placed in the computer.

d. Protection Against Other Malicious Software. Actions will be taken to reduce the vulnerability of WIN computers to other types of malicious software (e.g., trojan horses) by implementing the INFOSEC policies of this publication. In particular, implementation of a disciplined audit review program and adherence to the configuration management requirements of Joint Pub 6-03.11 will be accomplished. Site security personnel should be particularly sensitive to the methods of exploitation possible and take precautionary measures.

5. Responsibilities

a. DAAs. DAAs will ensure that:

(1) WIN personnel understand their responsibility to be familiar with the nature, variety, mechanisms, and effects of malicious software.

(2) Sufficient educational materials are available on the subject and accessible for users.

(3) Contingency plans include procedures for recovering from all degrees of malicious software attack. Backups will occur no less frequently than once per week.

(4) Attacks by malicious software are reported to the DISA.

(5) Workstations connected to their multiuser host have current antiviral software installed and operating where applicable.

b. DISA. The DISA will:

(1) Ensure that standard WIN software is distributed free of malicious software.

(2) Maintain a log of reported attacks against the WIN by malicious software.

(3) Immediately assess the potential for harm to the WIN upon being informed of a malicious software attack. If it is determined that other sites may be affected, the DISA will notify other site WASSOs of the attack with corrective actions to be taken.

c. WASSO. WASSOs will:

(1) Ensure that new users are adequately briefed on malicious software as part of their initial training.

(2) Receive current threat information as part of their required annual training.

(3) Ensure that antiviral software is distributed to WATASOs for installation.

(4) Immediately inform the DISA of a confirmed malicious software attack. Also, inform the site DAA, WSC, and the WASO.

(5) Prepare a report (see paragraph 6 of this chapter) on the results from the investigation resulting from a malicious software attack.

(6) Ensure that the malicious software attack report is forwarded to the WASO and DISA.

d. WATASO. WATASOs will:

(1) Ensure that workstation or terminal users have an adequate understanding of malicious software and know to notify the WATASO of a suspected attack.

(2) Immediately isolate a workstation from the WIN if an attack is suspected and notify the WASSO.

(3) Conduct an investigation if a malicious software attack occurs.

e. LAN Security Manager. LAN Security Managers will:

(1) Ensure that LAN workstation or terminal users have an adequate understanding of malicious software and know to notify the WATASO of a suspected attack.

(2) Immediately isolate a workstation from the LAN if an attack is suspected and notify the WASSO.

(3) In coordination with the WASSO (if different than the LAN Security Manager) and WATASO, conduct an investigation if a malicious software attack occurs on the LAN.

(4) Scan all software for malicious code before its installation on the LAN.

6. Reporting. Upon confirming that a malicious software attack has occurred, the WATASO, under the guidance of the WASSO, will conduct an investigation leading to a Malicious Software Attack Report. The report will present the facts associated with the attack to include the identity of the malicious software, its source, its impact on WIN operations, and eradication measures taken. Attacks against workstations or terminals will normally be handled as "FOR OFFICIAL USE ONLY." If the effects of the attack extend beyond a single workstation, its classification will be determined by the WASSO.

(INTENTIONALLY BLANK)

APPENDIX A

REFERENCES

1. Executive Documents

   a. Executive Order 12356, "National Security Information."

   b. Executive Order 12333, "United States Intelligence Activities."

   c. Public Law 100-235, "The Computer Security Act of 1987."

   d. OMB Circular No. A-130, "Management of Federal Information Resources."

   e. OMB Circular No. A-123, "Internal Control System."

   f. Title 18, United States Code 1905, "Espionage Act," Section 793, "Gathering, transmitting, or losing defense information," and Section 794, "Gathering or delivering defense information to aid foreign government."

   g. Information Security Oversight Office (ISOO) Directive No.1, "National Security Information."

   h. ISSO, "Information System Security Organization Strategic Plan."

   i. SM-769-89, "Procedures Manual for JCS Focal Point Communications Systems (U)."

   j. SM-684-88, "Policies and Procedures for Management of Command, Control, and Communications Systems."

   k. Federal Register 32 CFR Part 2003, "National Security Information; Standard Forms; Final Rule." Part II ISOO

2. Federal Information Pubs

   a. NIST Publications List 58, "Federal Information Processing Standards Publications (FIPS PUBS) Index."

   b. FIPS Pub 0, "General Description of the Federal Information Processing Standards Register."

   c. FIPS Pub 11-2, "Guideline: American National Dictionary for Information Processing Systems."

d. FIPS Pub 29-2, "Interpretation Procedures for Federal Information Processing Standards for Software."

e. FIPS Pub 31, "Guidelines for Automatic Data Processing Physical Security and Risk Management."

f. FIPS Pub 39, "Glossary for Computer Systems Security."

g. FIPS Pub 41, "Computer Security Guidelines for Implementing the Privacy Act of 1974."

h. FIPS Pub 46-1, "Data Encryption Standard."

i. FIPS Pub 48, "Guidelines on Evaluation of Techniques for Automated Personal Identification."

j. FIPS Pub 65, "Guideline for Automatic Data Processing Risk Analysis."

k. FIPS Pub 73, "Guidelines for Security of Computer Applications."

l. FIPS Pub 74, "Guidelines for Implementing and Using the NBS Data Encryption Standard."

m. FIPS Pub 81, "DES Modes of Operation."

n. FIPS Pub 83, "Guideline on User Authentication Techniques for Computer Network Access Control."

o. FIPS Pub 87, "Guidelines for ADP Contingency Planning."

p. FIPS Pub 88, "Guideline on Integrity Assurance and Control in Database Administration."

q. FIPS Pub 101, "Guideline for Lifecycle Validation, Verification, and Testing of Computer Software."

r. FIPS Pub 102, "Guideline for Computer Security Certification and Accreditation."

s. FIPS Pub 112, "Password Usage."

t. FIPS Pub 113, "Computer Data Authentication."

u. FIBS Pub 140, "General Security Requirements for Equipment Using The Data Encryption Standard."

3. DOD Documents (NSA, DIA, DNA, DLA, DISA)

a. Information Security

(1) DOD Directive 5200.1, "DoD Information Security Program."

(2) DOD Regulation 5200.1-R, "Information Security Program Regulation."

(3) DOD Directive 5200.12, "Conduct of Classified Meetings."

(4) DOD Directive 5200.21, "Dissemination of DoD Technical Information."

(5) DOD Directive 5215.2, "Computer Security Technical Vulnerability Reporting Program (SSTVRP)."

(6) DOD Directive 5230.9, "Clearance of DoD Information for Public Release."

(7) DOD Directive 5230.11, "Disclosure of Classified Military Information to Foreign Governments and International Organizations."

(8) DOD Directive C-5230.23, "Intelligence Disclosure Policy."

(9) DOD/ADUSD MEMORANDUM of 22 Sep 86, "Interpretation of the Two-Person Integrity Requirement of Paragraph 7-100b., DOD 5200.1-R, 'Information Security Program Regulation.'"

(10) DOD Directive 5230.24, "Distribution Statements on Technical Documents."

(11) DOD Instruction 7930.2, "ADP Software Exchange and Release."

(12) DOD Directive 5400.7, "DoD Freedom of Information Act Program."

(13) DOD Directive 5400.11, "Department of Defense Privacy Program (DA&M)."

(14) DOD Directive 7920.1, "Life-Cycle Management of Automated Information Systems (AISs)."

(15) C1-TR-001, "Computer Viruses: Prevention, Detection, and Treatment."

(16) NSA Catalog, "Information Systems Security - Products and Services Catalog."

(17) NSA/CSS Directive No. 10-27, "Security for Automated Information Systems and Networks (U)."

(18) NSA/CSS Manual 130-1, "NSA/CSS Operational Computer Security Manual."

(19) NSA/CSS Manual 130-2, "Media Declassification and Destruction Manual."

(20) CSC-STD-003-85, "Computer Security Requirements - Guidance for Applying the Department of Defense Trusted Computer System Evaluation Criteria in Specific Environments."

(21) CSC-STD-004-85, "Technical Rationale Behind CSC-STD-003-85: Computer Security Requirements - Guidance for Applying the Department of Defense Trusted Computer System Evaluation Criteria in Specific Environments."

(22) NCSC-TG-001, Version-2, "A Guide to Understanding AUDIT in Trusted Systems."

(23) NCSC-TG-002, "Trusted Product Evaluations - A Guide for Vendors."

(24) NCSC-TG-003, Version-1, "A Guide to Understanding DISCRETIONARY ACCESS CONTROL in Trusted Systems."

(25) NCSC-TG-004, Version-1, "GLOSSARY of Computer Security Terms."

(26) NCSC-TG-005, "Trusted NETWORK INTERPRETATION of The Trusted Computer System Evaluation Criteria."

(27) NCSC-TG-006, Version-1, "A Guide to Understanding CONFIGURATION MANAGEMENT in Trusted Systems."

(28) NCSC-TG-007, Version-1, "A Guide to Understanding DESIGN DOCUMENTATION in Trusted Systems."

(29) NCSC-TG-008, "Version-1, A Guide to Understanding TRUSTED DISTRIBUTION in Trusted Systems."

(30) NCSC-TG-009, Version-1, "Computer Security SUBSYSTEM Interpretation of the Trusted Computer System Evaluation Criteria."

(31) NCSC-TG-013, Version-1, "Rating Maintenance Phase - Program Document."

(32) NCSC-TG-014, Version-1, "Guidelines for Formal Verification Systems."

(33) NCSC-TG-015, Version-1, "A Guide to Understanding TRUSTED FACILITY MANAGEMENT."

(34) NCSC-TG-016, "Guideline for Writing Trusted Facility Manuals."

(35) NCSC-TG-017, Version-1, "A Guide to Understanding IDENTIFICATION AND AUTHENTICATION in Trusted Systems."

(36) NCSC-TG-019, Version-1, "Trusted Product Evaluation Questionnaire."

(37) NCSC-TG-020-A, Version-1, "Trusted UNIX Working Group (TRUSIX) Rationale for Selecting ACCESS CONTROL LIST Features for The UNIX System."

(38) NCSC-TG-021, Version-1, "TRUSTED DATABASE MANAGEMENT SYSTEM INTERPRETATION of Trusted Computer System Evaluation Criteria."

(39) NCSC-TG-022, Version-1, "A Guide to Understanding TRUSTED RECOVERY in Trusted Systems."

(40) NCSC-TG-025, Version 2, "A Guide to Understanding DATA REMANENCE in Automated Information Systems."

(41) NCSC-TG-026, Version-1, "A Guide to Writing the SECURITY FEATURES USER'S GUIDE for Trusted Systems."

(42) NCSC-TG-027, Version-1, "A Guide to Understanding Information System Security Officer Responsibilities for Automated Information Systems."

(43) NCSC-TG-028, Version-1, "Assessing Controlled Access Protection."

(44) NCSC C Technical Report 111-91, "Integrity-Oriented Control Objectives: Proposed Revisions to the Trusted Computer System Evaluation Criteria (TCSEC), DOD 5200.28-STD."

(45) NCSC C Technical Report 79-91, "Integrity in Automated Information Systems."

(46) NCSC-WA-002-85, "Personal Computer Security Considerations."

(47) DIA Manual 50-4 (C), "Security of Compartmented Computer Operations (U)."

(48) DCID 1/16, "Security Policy for Uniform Protection of Intelligence Processed in Automated Information Systems and Networks (U)."

(49) DCID 1/19, "Security Policy for Sensitive Compartmented Information."

(50) DISA Instruction 630-230-19, "Security Requirements for Automatic Data Processing Systems."

(51) DMA Manual 5200.28, "Automated Information Systems Security Requirements."

(52) DNA 5200.28D, "Security Requirements for Automated Information Systems (AISs)."

(53) DLA Regulation 5200.17, "Security Requirements for Automated Information and Telecommunications Systems."

b. Computer Security

(1) DOD Directive 5200.28, "Security Requirements for Automated Information Systems (AISs)."

(2) DOD Manual 5200.28-M, "ADP Security Manual" (under revision).

(3) DOD Standard 5200.28-STD, "Department of Defense Trusted Computer System Evaluation Criteria."

(4) NTISSAM COMPUSEC/1-87, "Advisory Memorandum of Office Automation Security Guideline."

c. Operational Security

(1) DOD Directive 5205.2, "DoD Operations Security Program."

(2) DOD Directive O-5205.7, "Special Access Program (SAP) Policy."

(3) DOD Directive 5205.8, "Access to Classified Cryptographic Information."

(4) DOD Directive 5210.2, "Access to and Dissemination of Restricted Data."

(5) DOD Directive 5210.50, "Unauthorized Disclosure of Classified Information to the Public."

(6) DOD Directive 5215.1, "Computer Security Evaluation Center."

(7) DOD Directive 5215.2, "Computer Security Technical Vulnerability Reporting Program (CSTVRP)."

(8) DOD Directive 3020.26, "Continuity of Operations Policies and Planning."

(9) DOD Directive 5100.30, "World-Wide Military Command and Control System (WWMCCS)."

(10) DOD Directive 5100.80, "World-Wide Military Command and Control System (WWMCCS) Evaluation Program."

(11) DOD Directive 5100.79, "World-Wide Military Command and Control System Engineer."

(12) CSC-STD-002-85, "Department of Defense Password Management Guideline."

(13) NSA/CSS Manual 130-1 , "The NSA/CSS Operational Computer Security Manual."

d. Communications Security and Emissions

(1) DOD Directive C-5200.5, "Communications Security (COMSEC) (U)."

(2) DOD Directive S-5200.17, "The Security, Use and Dissemination of Communications Intelligence (COMINT) (U)."

(3) DOD Directive S-5200.19, "Control of Compromising Emanations (U)."

(4) DOD Directive 5210.74, "Security of Defense Contractor Telecommunications."

(5) DOD Directive 5240.5, "DoD Technical Surveillance Countermeasures TSCM) Survey Program."

(6) DOD C-5030.58-M, "Defense Special Security Communications System; Security Criteria and Telecommunications Guidance."

(7) DCA Circular 370-D195-3, "DCS AUTODIN Category III Operational Acceptance Test."

(8) NACSIM 5100A, "Compromising Emanations Laboratory Test Requirements, Electromagnetics."

(9) NTISSP No. 300, "National Policy on Control of Compromising Emanations."

(10) NTISSI No. 3013, "Operational Security Doctrine for the Secure Telephone Unit III (STU-III) Type 1 Terminal."

(11) NTISSI No. 7000 (SECRET), "TEMPEST Countermeasures for Facilities (U)."

(12) NSA/CSS Regulation 90-5, "TEMPEST Security Program."

e. Personnel Security

(1) DOD Directive 5200.2, "DoD Personnel Security Program."

(2) DOD Regulation 5200.2-R, "DoD Personnel Security Program."

(3) DOD Directive 5220.6, "Defense Industrial Personnel Security Clearance Review Program."

(4) DCID 1/14, "Minimum Personnel Security Standards and Procedures Governing Eligibility for Access to Sensitive Compartmented Information."

f. Physical Security

(1) DOD Directive 5200.8, "Security of DoD Installations and Resources."

(2) DOD Directive 5220.22, "DoD Industrial Security Program."

(3) DOD Regulation 5220.22-R, "Industrial Security Regulation."

(4) DOD Manual 5220.22-M, "Industrial Security Manual for Safeguarding Classified Information."

(5) NACSIM 5203, "Guidelines for Facility Design and Red/Black Installation."

(6) DIA Manual 50-3, "Physical Security Standards for Construction of Sensitive Compartmented Information Facilities."

(7) NTISSP 200, "National Policy on Controlled Access Protection."

(8) DCID 1/12, "Intelligence Community Physical Standards for Sensitive Compartmented Information."

4. CJCS Documents

a. CJCS MOP 8, "Policy for Defense Switched Network Service."

b. CJCS MOP 50, "Command, Control, and Communications Master Plans, Assessments, and Evaluation."

c. CJCS MOP 60, "Release Procedures for Joint Staff and Joint Papers and Information."

d. MCJS-75-87, "Safeguarding the Single Integrated Operational Plan (SIOP) (U)."

5. Joint Staff Documents

a. Joint Pub 6-03.2, "Concept of Operations for the Minimum Essential Emergency Communications Network (U)."

b. Joint Pub 6-03.3, "WWMCCS Objective and Management Plan, WWMCCS Objectives (U)."

c. Joint Pub 6-03.4, "WWMCCS Objectives and Management Plan, WWMCCS Performance Criteria (U)."

d. Joint Pub 6-03.5, "WWMCCS Objectives and Management Plan, WWMCCS Composition (U)."

e. Joint Pub 6-03.6, "Doctrine for Joint WWMCCS Standards."

f. Joint Pub 6-03.7, "Security Policy for the WWMCCS Intercomputer Network."

g. Joint Pub 6-03.10, "WWMCCS Objectives and Management Plan, Management of the WWMCCS."

h. Joint Pub 6-03.11, "Management Procedures for the WWMCCS Standard ADP System and the WWMCCS Information System."

i. Joint Pub 6-03.12, "Policy for Modification and Improvement of the National Military Command System."

j. Joint Pub 6-03.13, "WWMCCS Evaluation Program (U)." This Joint Pub was canceled by a Joint Staff Memorandum of 16 Jan 1991.

k. Joint Pub 6-03.14, "Operation and Management of the WWMCCS Intercomputer Network."

l. Joint Pub 6-03.15, "Data Administration in the WWMCCS Information System."

m. Joint Pub 6-03.16, "WWMCCS Objectives and Management Plan, WWMCCS Concept of Operations (U)."

n. Joint Pub 6-03.17, "WWMCCS ADP Concept of Operations General Requirements for Post 1985."

6. Service Documents

a. Information Security

(1) AR 380-5, "Department of Army Information Security Program."

(2) AR 25-1, "The Army Information Resources Management Program."

(3) AFR 205-1, "Information Security Program."

(4) AFR 205-19, "Control of Dissemination of Intelligence Information."

(5) AFR 700-10, "Department of the Air Force, Information Systems: Information Systems Security."

(6) OPNAVINST 5510.1H, "Department of the Navy Information and Personnel Security Program Regulation."

(7) SECNAVINST 5239.2, "Department of the Navy Automated Information Systems (AIS) Security Program."

(8) NAVINTCOMINST 5239.3, "Department of the Navy SCI/Intelligence, Automated Information System (AIS) Security Program."

b. Computer Security

(1) AR 380-19, "Information Systems Security."

(2) AFR 205-16, "Computer Security Policy."

(3) AFR 56-32, "Computer Security for Operational Systems."

(4) AFR 56-31, "Computer Security for Acquisition and Development of Computer Systems."

(5) OPNAVINST 5239.1A, "Department of the Navy Automatic Data Processing Security Program."

(6) MCO Publication 5510.14, "Marine Corps Automatic Data Processing."

c. Operational Security

(1) AR 530-1, "Operations Security (OPSEC)."

(2) AFR 55-30, "Operations Security."

(3) AFR 57-1, "Operational Needs, Requirements, and Concepts."

(4) OPNAVINST 3070.1, "Operations Security."

d. Communication Security

(1) AR 380-53, "Communications Security Program."

(2) AFR 56-1, "Signal Security Policy."

(3) AFR 56-16, "TEMPEST Policy and Responsibilities."

(4) AFR 56-50, "Communications Security Policies, Procedures and Instructions."

(5) OPNAVINST C5510.93E, "Navy Implementation of National Policy on Control of Compromising Emanations."

e. Personnel Security

(1) AR 380-67, "The Department of the Army Personnel Security Program."

(2) AFR 205-32, "USAF Personnel Security Program."

f. Physical Security

(1) AR 190-13, "The Army Physical Security Program."

(2) AR 190-16, "Physical Security."

(3) AR 380-4, "DA Physical Security Program in the National Capitol Region."

(4) AR 380-49, "Industrial Security Program."

(5) AFR 205-4, "Industrial Security Program Regulation."

(6) OPNAVINST 5530.14B, "Department of the Navy Physical Security and Loss Prevention."

APPENDIX B

WIN SECURITY CLASSIFICATION GUIDE

1. Purpose. This appendix provides guidance and instructions on the classification of information involved with operation of the WIN. This appendix does not provide guidance for classification of user data files resident on WIN computers.

2. Authority. The authority for this guide is DOD Regulation 5200.1-R.

3. Classification Recommendations. Completely documented and justified recommendations for changes to this guide should be submitted to the Joint Staff, J-6, if any of the following conditions are met:

   a. If the instructions contained in this appendix impose requirements for protection that prove impractical.

   b. If current progress in a phase of a system, program, or project development, technological advances in the state of the art, changes in the international political situation, or other factors indicate a need for changes in the security classification guidance or policies described herein.

Pending final decision, the item(s) will be afforded a degree of protection equivalent to that of the current guidance or that recommended by the user, whichever is higher. All users of this guide are encouraged to assist in maintaining the currency and adequacy of the classification guidance furnished.

4. Regrading and Declassification Authority. This guide constitutes authority for regrading and declassifying information associated with the operation of the WIN, to include documents, photographs, equipment, and material. UNCLASSIFIED information, once communicated as such, may be classified or reclassified only as prescribed in DOD Regulation 5200.1-R.

5. Public Release

   a. The fact that this guide shows certain details of information to be unclassified does not allow automatic public release. Proposed public disclosures of unclassified information regarding the WIN will be submitted to the Joint Staff (WASO) for approval.

b. Only information already approved for public release may be released without further recourse. Information related to a public release developed after initial approval release must be submitted for review and processing as outlined above.

c. Approval for public release does not satisfy the export licensing requirements of the Departments of State and Commerce.

6. Release of Classified Information to Foreign Nationals. Information classified by this guide will not be released to foreign nationals, foreign governments, or international organizations without proper authorization in accordance with the national disclosure policy cited in DOD Regulation 5200.1-R.

TOPIC	DNGRADE/ CLASS	DECLASS	REMARKS
1. General	U		
a. General concepts of internetting.	U		
b. Overview of inter-netting functions (e.g., teleconferenc-ing, file transfer) and benefits of same.	U		
c. Network conuration.			Portions of network configuration may classification if they reveal classified information concerning a particular sensitive site’s functions.
d. The fact that the NMCS uses commercial and military communi-cations networks for contacting US forces deployed worldwide.	U		
e. Hardware configura-tion of the WIN.	U		An individual WIN site hardware configuration may be classified if required by local requirements.
f. Use and details of hardware components of the network.	U		

TOPIC	CLASS	DNGRADE/ DECLASS	REMARKS
2. Vulnerabilities or Threats			
a. Vulnerability of C3 functions carried out by the WIN to threats of alteration, sabotage interception, and intelligence exploit-ation if associated threat source material is quoted.	S-TS	OADR	Use the most restrictive marking of the source material. Classify TOP SECRET if vulnerability reveals an inability to accomplish the mission.
b. Vulnerability of WIN and its subsystems to physical attacks (including sabotage), electronic attacks, or nuclear effects with reference to specific nuclear weapons or their parameters (e.g., yield or fission and fusion ratio).	S-TS	OADR	Classify TOP SECRET if vulnerability reveals an inability to accomplish the mission or if appropriate source agency classification guidance dictates.
c. Vulnerability of primary WIN communications links, paths, or nodes to physical attacks (including sabotage), electronic attack, or nuclear effects with reference to specific nuclear weapons or their parameters (e.g., yield or fission and fusion ratio).	S-TS	OADR	Classify TOP SECRET if vulnerability reveals an inability to accomplish the mission or if appropriate source agency classification guidance dictates.
d. Specifications to improve network performance by counteracting identified threats if associated threat source is quoted.	S-TS	OADR	TOP SECRET if source data dictates.

TOPIC	DNGRADE/ CLASS	DECLASS	REMARKS
3. Survivability	S	OADR	Functional details may require higher classification.
a. Survivability of the WIN mission-critical functions (transattack and postattack).	S	OADR	
b. Survivability of the WIN sites against physical attacks (including sabotage), electronic attacks, or nuclear effects.	S-TS	OADR source agency	Refer to appropriate classification guidance. Classify TOP SECRET if an inability to accomplish mission is revealed.
c. Survivability of primary communications links, nodes, or paths of the WIN against physical attacks (including sabotage), electronic attacks, or nuclear effects.	S-TS	OADR source agency	Refer to appropriate classification guidance. Classify TOP SECRET if an inability to accomplish mission is revealed.
d. Survivability of nuclear and nonnuclear hardened communications equipment directly supporting the WIN.			
4. Disaster Recovery Plans			
Published plans for disaster prevention or recovery. Plans may include data, required actions, responsi-bilities, operating environment and location, hardware and software lists and configurations, and building layout.			UNCLASSIFIED unless more restrictive markings are dictated by source agency guidance or the compilation of material would dictate a higher classification.

TOPIC	CLASS	DNGRADE/ DECLASS	REMARKS
5. Continuity of Operations Plans			
In accordance with Joint Pub 6-03.14, WIN sites will submit copies of site contingency plans to the WIND.	C-S	OADR	Every effort should be made to keep these plans CONFIDENTIAL. However, if operational capabilities or procedures that exceed CONFIDENTIAL are to be included, then classification should not exceed SECRET.
6. Software			
a. Operating system software source code.	FOUO-TS		UNCLASSIFIED, unless it contains classified information as described in subparagraph IX-4a.
b. Applications Software.	U		UNCLASSIFIED unless source code contains classified information.
c. Details and specifics of security software.	U-TS	OADR	Same as 6a above.
7. Resource Access and Control			
a. WIN Logon Passwords.	S	OADR	Declassify when superseded.
b. WIN USERIDs.	U		
c. Project Account Passwords.	S	OADR	Same as 7a above.

TOPIC	CLASS	DNGRADE/ DECLASS	REMARKS
8. Performance Data and Reports			
a. Network technical performance data.	C	6 years	
Raw Data/Stats (60 days or more)	U		
Summary Data/Stats (No time limit)			
b. Network operational performance data.	C	6 years	
Raw Data/Stats (60 days or more)	U		
Summary Data/Stats (No time limit)	C-TS	6 years	Declassify after site returns to an operational mode.
c. Site outage forecasts for periods greater than 12 hrs.	C-TS	6 years	Minimum CONFIDENTIAL; higher based on any unresolved vulnerabilities documented in the report.
d. Risk Analysis Reports.	C-TS	6 years	Same as 7d above.
e. Requests for Waiver.	TS		Declassify based upon data contents.
f. WIN computer products (including magnetic and all printed media) when the actual classification of the contents of the product are not known and the product is to be transferred outside the organization or agency.			

TOPIC	DNGRADE/ CLASS	DECLASS	REMARKS
9. Priority Mode Messages			
a. Real-world crisis.	U-TS	OADR	Exercise specific.
b. Exercises.	U-TS	As stated in EXPLAN.	

(INTENTIONALLY BLANK)

APPENDIX C

DAA CERTIFICATION AND ACCREDITATION STATEMENT

NOTE: The sample shown below is a guide for submission of the DAA's statement of certification and accreditation as required in paragraph V-2.

From: DAA (Requesting)
To: DAA (Accrediting)
Subject: Certification of (system or facility name) to Create, Store, Process, and Use Sensitive or Classified Information or Equipment on the WIN

Ref: a. (Risk Analysis Report, ST&E Reports, etc.).
b. Joint Pub 6-03.7, pertinent Service, or Defense agency regulations.

1. I have carefully reviewed the results of the risk analysis, including the security test and evaluation of my site's computer system and its associated peripherals and all fixed and portable remote terminals. This site (fully or with the exceptions noted below) meets the security requirements and specifications detailed in Joint Pub 6-03.7.

2. This system fails to meet security specifications in the areas listed below. I have discussed associated risks, plans for improving security to meet specifications, and interim protection measures in the statements. (Reference here any applicable statements that contain detailed information on required changes and implementation schedules.)

3. I certify that I have carefully considered the above cited limitations, the threats and vulnerabilities that affect the operational requirements, and security measures that have been or will be implemented in physical, personnel, hardware, software, communications, and emanations security. I have determined that operation of the system is in the best interest of the (appropriate command) and that the security measures provided are reasonably adequate.

4. Accordingly, based on the risk analysis and the above cited limitations, I certify that this site is adequately secure to perform the missions and tasks for which it was designed. I accredit the site for local operations and request accreditation for operation in the WIN.

Signature Block

(INTENTIONALLY BLANK)

APPENDIX D

LOCAL DAA WAIVER

NOTE: This appendix provides a format for use by WIN site DAAs in approving waivers to Joint Pub 6-03.7 requirements. Appendix G indicates those requirements DAAs are authorized to waive. Site DAA waivers must be included in the site ST&E and RA to the Joint Staff.

STATEMENT OF WAIVER

1. I have carefully reviewed the requirement of paragraph XX.X of Joint Pub 6-03.7, and in accordance with the authority granted in Appendix G of Joint Pub 6-03.7, I waive the requirement. This waiver is granted for the following reason(s):

LIST REASONS

a. .....
b. .....

2. This waiver is valid through xx xxx xx (Day/Month/Year).

Signature Block of
Local DAA

(INTENTIONALLY BLANK)

APPENDIX E

RISK ANALYSIS REPORT

COVER SHEET

A. Organization or Agency and Address.
B. DAA (Name & Billet).
C. System Equipment (e.g., computer and operating system).
D. System Purpose or Use.
E. Accreditation History.
F. Date of Report.
G. Classification of Report and Reason for Classification.
H. Declassification Schedule.

EXECUTIVE SUMMARY

Narrative overview of significant observations. (Include a statement summarizing significant residual risk accepted.)

TABLE OF CONTENTS

(Outline and location of following information)

BODY OF REPORT

I Description of Risk Analysis

A. Risk Analysis assumptions; e.g., environment hostile or benign.
B. Description of risk analysis methodology used.

II Risk Analysis Team

A. Team organization (local, contractor, other Government agency, etc.).
B. Team composition (Team Members--Name, billet, phone number).
C. Team qualifications (e.g., formal training, OJT, types of access allowed, etc.).

III Background

A. Organization’s Mission.
B. Authority.
C. System’s Operational Requirements.
D. Security Objectives.
E. Security Incidents.

IV Site Description (What will be Risk Analyzed?)

A. Procedures, Plans or Other Directives.
B. Operations.
1. Training.
2. Systems Maintenance.
3. Emergence Destruction Plan.
4. COOP.
5. Disaster Recovery Plan.
6. Magnetic Media Control.
7. Declassification Procedures.
8. Procedures for Deployable Systems.
9. Other Related Activities.
C. Personnel (e.g., personnel security and access programs).
D. Physical:
1. Environment.
a. Geography.
b. Climate.
c. Geology.
(1) Ground Composition.
(2) Earthquake Vulnerability.
2. Public Services Available.
3. Other Services.
4. Structure of Computer Facility.
E. Communications.
F. Emanations.
G. Hardware.
H. Software.
I. Support Organizations.
1. Administrative Support.
2. Local Security Office.
3. Provost Marshal/Master-at-Arms.
J. Assests/Critical Resources (Prioritized).
1. Facilities.
2. Personnel.
3. Hardware.
4. Software.
5. Information.
6. Administrative Information.
K. Connected AISs (Attach Accreditation letters & MOAs).
L. Site Physical Configuration Diagram.

V Risk Analysis and ST&E

A. Scope and Objectives.
B. General Approach.
C. Data Collection (How was it done? Questionnaires, interviews, walkthroughs?).

VI Risk Analysis Results

A. Completed Appendix G Checklist.

B. Results of Risk Analysis.
1. Assets.
2. Threats.
3. Vulnerabilities to Threats.
4. Safeguards.
5. ST&E of Safeguards (evaluate safeguards applied to vulnerabilities).
a. Safeguard #1:
(1) Threat Countered by Safeguard
(2) Description of Safeguard Functionality
(3) Test Description
(4) Results:
(a) Safeguard Functionality
(b) Safeguard Assurance
b. Safeguard #2:
(1) Threat Countered by Safeguard
(2) Description of Safeguard Functionality
(3) Test Description
(4) Results:
(a) Safeguard Functionality
(b) Safeguard Assurance
c. Etc.
C. Summary of Residual Risks.

VII Evaluation and Recommendations

A. Overview of General Findings.
B. Specific Recommendations.
1. Procedures.
a. Administrative: The following administrative procedures need to be developed:
(1) Procedure:
DAA Directed Approach:
Suspense:
(2) Procedure:
DAA Directed Approach:
Suspense:
(3) etc.
(b) Operational: The following operational procedures need to be developed:
(1) Procedure:
DAA Directed Approach:
Suspense:
(2) Procedure:
DAA Directed Approach:
Suspense:
2. Personnel (Address relevant recommendations.).
3. Physical (Address relevant recommendations.).
4. Communications (Address relevant recommendations.).
5. Emanations (Address relevant recommendations.).
6. Hardware (Address relevant recommendations.).
7. Software (Address relevant recommendations.).

8. Information/Data (Address relevant recommendations.).
9. Security Training (Address relevant recommendations.).
10. Contingency Planning (Address relevant recommendations.).

VIII Enclosures

A. Mulituser Host Accreditation Letter.

B. Local DAA Waivers (See Appendix D for format.).

C. Connected AIS Documentation:

1. MOA.
2. Stand-Alone accreditation letter.
3. Letter accrediting connection of AIS to WIN host.

NOTE: Repeat paragraph C for each connected AIS.

(INTENTIONALLY BLANK)

APPENDIX F

TWO-PERSON STAFFING BACKGROUND

NOTE: This memorandum was retyped verbatim from OSD memorandum of 22 Sep 1986 to provide background information on the "Two Person Staffing" requirement of Chapter VII, paragraph 3 of this publication. It is provided below.

MEMORANDUM FROM ASSISTANT DEPUTY SECRETARY OF DEFENSE (COUNTERINTELLIGENCE AND SECURITY)

Subject: Interpretation of the Two-Person Integrity Requirement of Paragraph 7-100b., DOD 5200.1-R, "Information Security Program Regulation"

Numerous questions with respect to implementation of the Two-Person integrity requirements of paragraph 7-100b, DOD 5200.1-R, concerning working with TOP SECRET information or information controlled within Special Access Programs prompted this memorandum.

In making its recommendation (#32) to the Secretary of Defense, the Stilwell Commission intended that employees not be permitted to work alone in areas where TOP SECRET or Special Access Program information is stored. The commission's primary concern was with persons working unsupervised in such areas on weekends or after normal duty hours. But the Commission recognized a need for waiving this requirement in many instances and this recommendation (paragraph 7-100 b., DOD 5200.1-R) provides, in fact, that DOD components may delegate the authority to approve such waivers to whatever level is deemed appropriate.

In general, it is not intended that implementation of this requirement should place undue burdens on mission accomplishment, nor result in excessive expenditures for new security equipment. Accordingly, the following guidance is provided:

To begin with, this requirement should not be referred to as the "two-man rule," which tends to evoke comparisons with Two-Person requirements in the nuclear weapons community. There is no intent to create a rigidly enforced "no lone zone" around TOP SECRET information.

There is no intent that the second person necessarily have equal access to and knowledge of the information that is accessible only to the first person. The second person might have a SECRET clearance, and be denied actual knowledge of the TOP SECRET or Special Access Program

information, but function effectively in the second person role provided that person is aware of his or her responsibility to provide enhanced protection for the information. However, it is recognized that there will be circumstances where both people must have equal access.

To mitigate the impact of the Two-Person integrity requirements, it should be possible, in many circumstances, to withdraw TOP SECRET material from most people and place such material in the direct custody of TOP SECRET Control Officer. Then, offices served by the TSCO do not have to be concerned about implementation of rule except when, for example, an action officer checks out a TOP SECRET document from the TSCO for use during nonduty hours. The collateral security benefits of such a procedure are obvious.

In most cases, it would not be proper to increase the number of personnel granted access to a Special Access Program merely to comply with the Two-Person integrity rule; a waiver would be more appropriate.

Implementation of Two-Person integrity rule in a computer environment may pose special problems, especially when a system with remote terminals is operated in a TOP SECRET system high mode. There is not intent that implementation of the rule cause a doubling of staffing requirements. Moreover, implementation should not cause operation hours of, for example, a communications center, to be reduced.

There is no intent to apply the rule to local courier operations unless other factors are present such as Sensitive Compartmented Information. Application of the rule to the operations of the Armed Forces Courier Service will be determined during the ongoing review of that Service under auspices of the Deputy Under Secretary of Defense (Policy).

Two-Person integrity rule does not apply to NATO or CNWDI information as these classes information are essentially excluded from the provisions of Chapter XIX, DOD 5200.1-R.

It is not essential that two persons be able to see each other at all times in order to comply with the spirit of the Two-Person integrity rule.

As was agreed during the 5 August 1986 meeting of the Defense Information Security Committee, a waiver of the Two-Person integrity rule would not be required for those circumstances where one person works alone in a compartment on a naval vessel while at sea. In such circumstances,

compensatory measures should be adopted and are inherently present. For example, being at sea limits the opportunity for unauthorized removal of the information in question. This, in combination with a random inspection program in accordance with Section 3, Chapter V, DOD 5200.1-R, upon arrival in port, should provide the enhanced protection which is the underlying reason for the Two-Person integrity rule.

One other way of implementing the Two-Person integrity rule that is being considered by some is to procure replacement control drawers with dual built-in combination locks for existing security containers approved by the General Services Administration (GSA). Such replacement drawers would cost approximately $300 - $500, depending on brand. For such equipment to be effective, no one person can be permitted to access to both combinations; two authorized persons would be required to open the safe; and both would have to maintain the Two-Person integrity rule until the material is fully secured. While use of double-locked safes may be desirable in some circumstances, such as where a large volume of TOP SECRET or Special Access Program material is stored, widespread purchasing of such safes would be a relatively expensive implementation of the new requirement in most offices.

In summary, it is clear that too rigid an implementation of the Two-Person requirement will lead to unintended costs both in terms of operational efficiency and unnecessary security equipment and devices. The object of the new policy is to establish better control over specially sensitive information, particularly during nonwork hours. So long as supervisory officials at appropriate levels are aware of, and approve, exceptions to the general requirement, then its intent has been satisfied.

L. Britt Snider
Assistant Deputy Under Secretary of Defense
(Counterintelligence and Security)

Attachment

OSD: Policy POC for 5200.1-R
Mr. David E. Whitman, AV 225-2289, Room: 3C274
Assistant for Info & Tech Security
Dep Dir Info & Tech Security
Dep Under Sec for Security Policy

(INTENTIONALLY BLANK)

APPENDIX G

WIN SECURITY CHECKLIST

CHAPTER I

GENERAL PROVISIONS

(Y) (N) (WA)

1. Scope

a. Security policy applicable to non-WIN AISs connected to the WIN is documented in an MOA signed by both the WIN multiuser host DAA and the DAA of the connected non-WIN AIS. MOAs are prepared in the format of and contain the minimum information of Appendix J of this publication. (I-3a(1) & 3b(2))

( ) ( ) NW

b. If two WIN sites covered by different Service or Defense agency security policies are involved, either the more stringent will apply or the two DAAs may sign an MOA whose security policy is at least as stringent as Joint Pub 6-03.7. (I-3a(2))

( ) ( ) NW

c. CINC WIN sites will either comply with their supporting Service ADP security regulation (e.g., AR 380-19) or prepare a CINC-approved regulation as stringent as the applicable Service regulation. If the latter, the J-6, Joint Staff will be placed on the distribution list. (I-3a(3))

( ) ( ) NW

NOTE: WA--Waiver Authority. Waivers to this document may be approved by:

(S) - the local site DAA
(J) - Joint Staff
(NW) - nonwaiverable
Y = Yes; N = No.
Numbers in parentheses refer to paragraphs in this publication.

2. Requests for Waiver

a. Current site DAA waivers will be documented in the Risk Analysis report. (I-7a)
( ) ( ) NW

b. Alternative protection methods will be provided to safeguard information affected by the waiver. (I-7f)
( ) ( ) J

c. Identify connections to other systems or networks. Identify effects this waiver may have on security safeguards implemented on those systems. (I-7h)
( ) ( ) NW

d. Waiver requests will be reviewed and signed by the WASSO or WASSM of the submitting organization. (I-7j)
( ) ( ) NW

3. Security Incident Reports

a. Security incidents are investigated in accordance with Service or Defense agency directives to determine their cause and the corrective action(s) to be taken. (I-8a)
( ) ( ) J

b. Incidents caused by a failure of WIN standard and nonstandard hardware or software will be reported in accordance with Joint Pub 6-03.11. (I-8a)
( ) ( ) J

c. Incidents affecting two or more WIN multiuser host sites will be reported to the WASO. (I-8a)
( ) ( ) NW

NOTE: WA--Waiver Authority. Waivers to this document may be approved by:

(S) - the local site DAA
(J) - Joint Staff
(NW) - nonwaiverable
Y = Yes; N = No.
Numbers in parentheses refer to paragraphs in this publication.

d. If compromise of classified information has occurred, a report of facts surrounding the incident will be immediately forwarded to a responsible official with a copy to the WASO. A preliminary inquiry will then be conducted in accordance with DOD 5200. 1-R. (I-8a)

( ) ( ) NW

e. The WASSO will immediately inform the affected OPRs of significant security incidents (Chapter I, subparagraphs 8b(2) and (3)) that involve their files. (I-8c)

( ) ( ) NW

CHAPTER II

RESPONSIBILITIES

4. Terminal Area Certification Authority or DAA. Site DAAs must assign either a Terminal Area Certification Authority or a Terminal Area DAA for each WIN terminal area. (II-11)

( ) ( ) NW

5. WWMCCS ADP Terminal Area Security Officer. Each organization responsible for a terminal area will appoint a WATASO. The WATASO, working in conjunction with the supporting multiuser host WASSO, is responsible for implementing procedures designed to control access to remote devices. The WATASO serves as the primary POC for terminal-related security matters. (II-12)

( ) ( ) NW

6. Users

a. Protect their logon passwords as described in Chapter XII, paragraph 2. Users should change their passwords

NOTE: WA--Waiver Authority. Waivers to this document may be approved by:

(S) - the local site DAA
(J) - Joint Staff
(NW) - nonwaiverable
Y = Yes; N = No.
Numbers in parentheses refer to paragraphs in this publication.

immediately upon receipt from their WASSO or WATASO. (II-16a)

( ) ( ) J

b. Protect classified and other sensitive materials as specified in Chapter XVI. In particular, users will: (II-16b)

(1) Not leave active computer terminals unattended. (II-16b(1))

( ) ( ) J

(2) Review system output, including continuity of page numbering. (II-16b(2))

( ) ( ) J

(3) Ensure that output products, including copies of CRT displays, are appropriately marked and initiate formal accountability for TOP SECRET documents as required by Chapter XVI. (II-16b(3))

( ) ( ) J

(4) Appropriately mark ADP storage devices TOP SECRET (unless they have been downgraded) and maintain an inventory of ADP storage devices in the user's custody. See Chapter XVI for details. (II-16b(4))

( ) ( ) J

(5) Follow restrictions on the copying and use of copyrighted and licensed software. In particular, the user will not make copies for private use or use software outside the license agreement. (II-16b(5))

( ) ( ) J

NOTE: WA--Waiver Authority. Waivers to this document may be approved by:

(S) - the local site DAA
(J) - Joint Staff
(NW) - nonwaiverable
Y = Yes; N = No.
Numbers in parentheses refer to paragraphs in this publication.

(6) Give file permissions based on the least privilege concept. (See Glossary.) (II-16b(6))
( ) ( ) J

c. Report security-related discrepancies. Elements or components of an ADP system will function in a cohesive, identifiable, predictable, and reliable manner so that malfunctions can be detected and reported in time to prevent or minimize disruption of the system. Accordingly, the user will report security-related discrepancies to the WASSO or to the WASSO's designated representative; e.g., WATASO. (II-16c)
( ) ( ) J

CHAPTER III

WIN SITE SECURITY, AIS INTERFACES, AND LANs

7. Security Operating Mode. The WIN operates in the system high security mode at the TOP SECRET classification level; i.e., it is a TOP SECRET system high AIS. (III-2)
( ) ( ) J

8. AIS Connections. AISs connected to the WIN will be accredited to operate at US TOP SECRET unless:

a. The SDN requesting approval for connection of the AIS to the WIN will show that WIN data passed to the AIS has been reliably downgraded to the classification level at which that AIS is accredited. (III-3a(1))
( ) ( ) J

b. Users on AISs accredited below US TOP SECRET are not allowed to logon to the WIN. (III-3a(1))
( ) ( ) J

NOTE: WA--Waiver Authority. Waivers to this document may be approved by:

(S) - the local site DAA
(J) - Joint Staff
(NW) - nonwaiverable
Y = Yes; N = No.
Numbers in parentheses refer to paragraphs in this publication.

c. If the connected AIS is accredited to operate at US TOP SECRET and at one or more classification levels less sensitive than US TOP SECRET, SDN approved hardware or software or procedures will be in place to ensure that only users with a US TOP SECRET clearance granted formal access to the WIN, can access the WIN. (III-3a(2))
( ) ( ) J

d. Workstations accredited to operate in the MLS mode will comply with the security policy requirements of Joint Pub 6-03.7 during those periods when they are used for WIN connectivity. (III-3a(2))
( ) ( ) J

e. If the connected AIS is accredited to operate with SCI, the SDN requesting approval of the connection will show that data from the AIS transferred to the WIN is sanitized of all SCI. (III-3a(2))
( ) ( ) J

f. All connections of AISs to the WIN will be preapproved by SDN in accordance with Joint Pubs 6-03.7 and 6-03.11. (III-3b)
( ) ( ) J

g. If an MLS Guard is required, a risk index is calculated in accordance with DODD 5200.28 Encl (4). (III-3b(3))
( ) ( ) J

h. Documentation accompanies the SDN to support and validate all aspects of the system's security function as agreed to jointly by the DAAs signing the MOA and approved by the WIN DAA. (III-3b(3))
( ) ( ) J

NOTE: WA--Waiver Authority. Waivers to this document may be approved by:

(S) - the local site DAA
(J) - Joint Staff
(NW) - nonwaiverable
Y = Yes; N = No.
Numbers in parentheses refer to paragraphs in this publication.

i. All documents associated with the SDN will be filed with the WIN multiuser host's current accreditation documentation. (III-3c)
( ) ( ) J

9. LANs

a. Connection of WIN LANs to the WIN are approved by SDN in accordance with Joint Pubs 6-03.7 and 6-03.11 before connection. (III-4a)
( ) ( ) J

b. Accreditation. WIN LANs will have a DAA appointed in writing and will be accredited by the DAA to process collateral TOP SECRET information independently of the WIN multiuser host to which it is attached. WIN LANs will, at a minimum, possess the functionality of a C2 TCSEC AIS. (III-5a)
( ) ( ) J

c. The SDN will include a Risk Analysis of the LAN and interface to the WIN to show that necessary safeguards have been sufficiently tested to assure they provide an acceptable level of trust to the DAAs concerned. (III-5b)
( ) ( ) J

d. If a WIN LAN is to be connected to a WIN multiuser host under the authority of a different Service with different security requirements than the multiuser host, an MOA between the LAN and host DAAs has been written. (III-5d)
( ) ( ) J

e. WIN LANs have a DAA appointed in writing and are accredited by the DAA to process collateral TOP SECRET information

NOTE: WA--Waiver Authority. Waivers to this document may be approved by:

(S) - the local site DAA
(J) - Joint Staff
(NW) - nonwaiverable
Y = Yes; N = No.
Numbers in parentheses refer to paragraphs in this publication.

independently of the WIN multiuser host to which it is attached. (III-6a)
( ) ( ) J

f. WIN LANs, at a minimum, possess the functionality of a C2 TCSEC AIS. (III-6a)
( ) ( ) J

g. Each LAN user will be uniquely identified and authenticated at initial logon to his or her workstation. In addition, each LAN user will be uniquely identified and authenticated to all LAN resources to which he or she has access either by the resource or through a controlling processor which mediates access to the resource. (III-6b(1))
( ) ( ) J

h. All LAN resources will be uniquely identifiable to all other LAN resources either directly or indirectly through a controlling processor. (III-6b(2))
( ) ( ) J

i. Minimum LAN Audit Requirements. At a minimum, the following events will be audited (III-6h):

(1) Startup and shutdown. (III-6h(1))
( ) ( ) J

(2) Logon and logoff. (III-6h(2))
( ) ( ) J

(3) Object create, modify, or delete. (III-6h(3))
( ) ( ) J

NOTE: WA--Waiver Authority. Waivers to this document may be approved by:

(S) - the local site DAA
(J) - Joint Staff
(NW) - nonwaiverable
Y = Yes; N = No.
Numbers in parentheses refer to paragraphs in this publication.

CHAPTER IV

WIN SITE SECURITY ADMINISTRATION

10. WWMCCS ADP System Security Officer (WASSO)

a. Individual appointed in writing. (IV-3a)
( ) ( ) J

b. WASSO has direct access to the multiuser host or RNP DAA. (IV-3c)
( ) ( ) S

c. US Government employee. (IV-3d)
( ) ( ) J

d. The WASSO's personal technical qualifications or the technical qualifications represented by available site personnel directly supporting the WASSO's security functions will include, at a minimum (IV-3d):

(1) Experience in computer operations. (IV-3d(1))
( ) ( ) S

(2) Completion of a basic computer security course of instruction. (IV-3d(2))
( ) ( ) J

(3) Completion of a WIN specific security course of instruction. (IV-3d(3))
( ) ( ) J

(4) Completion of a system software programmers course. (IV-3d(4))
( ) ( ) S

(5) Experience as a systems software analyst or programmer on a WIN

NOTE: WA--Waiver Authority. Waivers to this document may be approved by:

(S) - the local site DAA
(J) - Joint Staff
(NW) - nonwaiverable
Y = Yes; N = No.
Numbers in parentheses refer to paragraphs in this publication.

multiuser host computer or equivalent. (IV-3d(5)

( ) ( ) S

(6) Experience in the application and enforcement of information and ADP security measures and countermeasures to security threats and vulnerabilities. (IV-3d(6))

( ) ( ) S

e. WASSO responsibilities (IV-3e):

(1) Develop, review, revise, and submit for approval procedures for reporting, investigating, and resolving all WWMCCS ADP System security incidents involving the site. (IV-3e(1))

( ) ( ) J

(2) Ensure that all personnel who install, operate, maintain, or use the WIN hold the proper security clearance and access authorization and are indoctrinated by their respective security officer in applicable security requirements and responsibilities. (IV-3e(2))

( ) ( ) J

(3) Supervise review of security audit information. (IV-3e(3))

( ) ( ) J

(4) Develop, review, revise, submit for approval, and implement procedures for monitoring and reacting to security warning messages and reports. (IV-3e(4))

( ) ( ) J

NOTE: WA--Waiver Authority. Waivers to this document may be approved by:

(S) - the local site DAA
(J) - Joint Staff
(NW) - nonwaiverable
Y = Yes; N = No.
Numbers in parentheses refer to paragraphs in this publication.

(5) Formulate procedures for WIN physical and personnel access controls. (IV-3e(5))
( ) ( ) J

(6) Participate in system malfunction analyses and participate in preparing incident reports. (IV-3e(6))
( ) ( ) J

(7) Evaluate site software patches made to WIN standard operating system software to ensure these patches do not create security vulnerabilities. (IV-3e(7))
( ) ( ) J

(8) Evaluate the effectiveness and impact of the security measures and procedures of any connection of the WIN site elements with other systems (e.g., DSN) and assist in preparing an SDN, SCP, or correspondence to the appropriate command authority or DAA identifying problem areas as appropriate. (IV-3e(8))
( ) ( ) J

(9) Report security incidents that could damage network security to the appropriate command authority or DAA for consideration and appropriate action; e.g., compliance with the Computer Security Technical Vulnerability Reporting Program prescribed by DODI 5215.2. (IV-3e(9))
( ) ( ) J

(10) Immediately notify the appropriate command authority or site DAA of any suspected security incident associated with a

NOTE: WA--Waiver Authority. Waivers to this document may be approved by:

(S) - the local site DAA
(J) - Joint Staff
(NW) - nonwaiverable
Y = Yes; N = No.
Numbers in parentheses refer to paragraphs in this publication.

subordinate network site. Provide recommendations to assist the site DAA in determining if other sites should be denied access to resources at the DAA's site and if network operations should be terminated at the DAA's site. The WASSO will be notified of actions taken by the command or DAA. (IV-3e(10))

( ) ( ) J

(11) Prepare necessary directives that implement WIN or site DAA prescribed security measures to be used at each site installation and monitor their application. (IV-3e(11))

( ) ( ) J

(12) Maintain documentation detailing the site hardware and software configuration and all security countermeasures that protect it from attacks. (IV-3e(12))

( ) ( ) J

(13) Ensure that inspections are conducted as required by this publication or applicable Service or Defense agency directives. (IV-3e(13))

( ) ( ) J

(14) Maintain files on current Risk Analysis with Accreditation letters and related documentation. Included will be all waiver-related documentation. (IV-3e(14))

( ) ( ) J

NOTE: WA--Waiver Authority. Waivers to this document may be approved by:

(S) - the local site DAA
(J) - Joint Staff
(NW) - nonwaiverable
Y = Yes; N = No.
Numbers in parentheses refer to paragraphs in this publication.

(15) Conduct system audits, verifications, and acceptance checks and maintain documentation on the results. (IV-3e(15))
( ) ( ) J

(16) Conduct random checks to verify compliance with the security procedures and requirements of this publication. (IV-3e(16))
( ) ( ) J

(17) Evaluate the security impact of proposed site-unique modifications to software and approve those that do not adversely affect security. Request prior approval from the WIN DAA of all site-unique modifications to software that affect other WIN sites. (IV-3e(17))
( ) ( ) J

(18) Periodically monitor system use. With the site commander's or designated DAA authorization, inspect and monitor user files for possible security problems. (IV-3e(18))
( ) ( ) J

(19) Represent the site at meetings concerning WIN security. (IV-3e(19))
( ) ( ) S

(20) Coordinate WIN STPs. (IV-3e(20))
( ) ( ) J

(21) Perform WASSM-related duties when a WASSM is not appointed. (IV-3e(21))
( ) ( ) J

(22) Review security impact of SDNs, or SCPs in accordance with Joint Pub

NOTE: WA--Waiver Authority. Waivers to this document may be approved by:

(S) - the local site DAA
(J) - Joint Staff
(NW) - nonwaiverable
Y = Yes; N = No.
Numbers in parentheses refer to paragraphs in this publication.

6-03.11 before their submission to the DOD Component or the Joint Staff for approval. Provide separate signed statement of review as part of the SDN or SCP submission. (IV-3e(22))
( ) ( ) J

(23) Identify security requirements and manage access in relationship to remote AISs that afford multiuser connections into the WIN. (IV-3e(23))
( ) ( ) J

11. WWMCCS ADP Terminal Area Security Officer (WATASO)

a. WATASO appointed in writing. (IV-4b)
( ) ( ) J

b. WATASO serves as the single point of contact at the terminal area. (IV-4b)
( ) ( ) S

c. The WATASO will have direct access to the terminal area certification authority or DAA. (IV-4b)
( ) ( ) S

d. The WATASO must be a WIN user. (IV-4b)
( ) ( ) S

e. US Government Employee. (IV-4c)
( ) ( ) J

f. Personal Technical Qualifications:

(1) Experience in computer operations on a stand-alone workstation, minicomputer, or mainframe computer. (IV-4c(1))
( ) ( ) J

NOTE: WA--Waiver Authority. Waivers to this document may be approved by:

(S) - the local site DAA
(J) - Joint Staff
(NW) - nonwaiverable
Y = Yes; N = No.
Numbers in parentheses refer to paragraphs in this publication.

(2) Completion of a basic INFOSEC course of instruction. (IV-4c(2))
( ) ( ) J

(3) Completion of a WIN-specific security course of instruction. (IV-4c(3))
( ) ( ) J

(4) If responsible for multiuser intelligent workstations, the WATASO must have attended a system administrator's course of instruction for that workstation. (IV-4c(4))
( ) ( ) J

g. WATASO Duties. (IV-4d)

(1) Assist the WASSO in preparing terminal security procedures. (IV-4d(1))
( ) ( ) S

(2) Implement approved security procedures. (IV-4d(2))
( ) ( ) J

(3) Maintain a current access list of personnel authorized access to the remote device(s). (IV-4d(3))
( ) ( ) J

(4) Report security abnormalities to the WASSO or a designated representative. (IV-4d(4))
( ) ( ) J

(5) Safeguard and return to the WASSO or a designated representative all ADP products that cannot be identified or that contain extraneous data. (IV-4d(5))
( ) ( ) J

NOTE: WA--Waiver Authority. Waivers to this document may be approved by:

(S) - the local site DAA
(J) - Joint Staff
(NW) - nonwaiverable
Y = Yes; N = No.
Numbers in parentheses refer to paragraphs in this publication.

(6) Conduct random checks to ensure that the security procedures and requirements of this publication for the terminal area are being followed. (IV-4d(6))
( ) ( ) J

(7) Issue the initial password to approved users of workstations requiring workstation logon passwords in addition to multiuser host logon passwords. (IV-4d(7))
( ) ( ) J

(8) Maintain and review appropriate audit files residing on workstations with audit capabilities. (IV-4d(8))
( ) ( ) J

(9) Serve as the workstation administrator for intelligent workstations within his or her terminal area. (IV-4d(9))
( ) ( ) J

12. LAN Security Manager

a. Individual appointed in writing. (IV-5a)
( ) ( ) J

b. LAN Security Manager will have direct access to the LAN DAA. (IV-5a)
( ) ( ) J

c. US Government Employee. (IV-5b)
( ) ( ) J

d. The LAN Security Manager will have completed a LAN administrator's course for the LAN being managed. (IV-5b)
( ) ( ) J

NOTE: WA--Waiver Authority. Waivers to this document may be approved by:

(S) - the local site DAA
(J) - Joint Staff
(NW) - nonwaiverable
Y = Yes; N = No.
Numbers in parentheses refer to paragraphs in this publication.

e. LAN Security Manager Duties: (IV-5c)

(1) Prepares LAN security procedures. (IV-5c(1))
( ) ( ) J

(2) Implements approved LAN security procedures. (IV-5c(2))
( ) ( ) J

(3) Establishes LAN user accounts. (IV-5c(3))
( ) ( ) J

(4) Manages LAN USERIDs and passwords. (IV-5c(4))
( ) ( ) J

(5) Maintains LAN access controls. (IV-5c(5))
( ) ( ) J

(6) Conducts random checks to ensure that security procedures and requirements of this publication for the LAN are being followed. (IV-5c(6))
( ) ( ) J

(7) Performs routine real-time security functions; e.g., denying access based on security violations. (IV-5c(7))
( ) ( ) J

(8) Analyzes LAN audit reports. (IV-5c(8))
( ) ( ) J

(9) Ensures correct function of LAN backups. (IV-5c(9))
( ) ( ) J

NOTE: WA--Waiver Authority. Waivers to this document may be approved by:

(S) - the local site DAA
(J) - Joint Staff
(NW) - nonwaiverable
Y = Yes; N = No.
Numbers in parentheses refer to paragraphs in this publication.

CHAPTER V

ACCREDITATION, CERTIFICATION AND RISK MANAGEMENT

13. DAA. The DAA is the accrediting authority and will be appointed in writing. (V-1b)

( ) ( ) NW

14. Accreditation. The WIN multiuser host or remote AIS (RNPs, LANs, etc.) will be accredited for stand-alone operations. Furthermore, each WIN multiuser host will be accredited to operate in the WIN; i.e., the host's connection to the WIN will be accredited by the WIN DAA. The certification and accreditation process for both stand-alone operations and connection to the WIN will be repeated once every 3 years. (V-1d(2))

( ) ( ) NW

CHAPTER VI

ADP SECURITY TRAINING AND AWARENESS

15. Training Program

a. Each WIN multiuser host DAA will establish an INFOSEC training program in accordance with Chapter VI, paragraph 1. (VI-1)

( ) ( ) NW

b. WIN users will receive the training in paragraph 1 of this chapter initially, and as frequently as required, by their respective Service regulations. Training will occur at least once every 12 months. (VI-2)

( ) ( ) J

NOTE: WA--Waiver Authority. Waivers to this document may be approved by:

(S) - the local site DAA
(J) - Joint Staff
(NW) - nonwaiverable
Y = Yes; N = No.
Numbers in parentheses refer to paragraphs in this publication.

c. The WIN multiuser host DAA will ensure that the WIN security staff at all levels is adequately trained to perform the security role as required by this publication and applicable DOD, Service, and Defense agency regulations. (VI-3)
( ) ( ) J

CHAPTER VII

PERSONNEL SECURITY

16. Personnel Security

a. Personnel who have unescorted access to TOP SECRET WIN areas will have an interim or final US TOP SECRET clearance. In addition, personnel requiring access to WIN information will have been granted access to the WIN based upon a need to know for specific data on the WIN. (VII-1)
( ) ( ) J

b. Personnel who do not possess the proper clearance must be escorted by properly cleared WIN personnel while in the WIN area. (VII-1)
( ) ( ) J

c. Contractors who have WIN access must have an interim or final US TOP SECRET clearance and have a need to know for some data on the WIN. (VII-2a)
( ) ( ) J

d. Contractors who maintain hardware connected to the WIN must possess a US TOP SECRET clearance. (VII-2b)
( ) ( ) S

NOTE: WA--Waiver Authority. Waivers to this document may be approved by:

(S) - the local site DAA
(J) - Joint Staff
(NW) - nonwaiverable
Y = Yes; N = No.
Numbers in parentheses refer to paragraphs in this publication.

e. A record of all contractor maintenance visits to WIN areas will be made and retained for 24 months. (VII-2c)
( ) ( ) J

f. Contractors will not serve as WASSMs or WASSOs, LAN Security Managers, WATASOs, TP8 Administrators, or LAN Security Managers and will not be given administrator privileges. (VII-2d)
( ) ( ) S

g. All operational WIN multiuser hosts that require staffing must be manned by at least two appropriately cleared personnel. (VII-3)
( ) ( ) J

h. Foreign nationals will not have access to WIN software or data resources as users or maintenance personnel without the WIN DAA approval. (VII-4)
( ) ( ) J

i. Foreign nationals will not install, repair, or maintain WIN hardware. (VII-4)
( ) ( ) S

j. Foreign nationals will not serve as WASSMs, WASSOs, WATASOs, WSCs, TP8 Administrators, or LAN Security Managers. (VII-4)
( ) ( ) J

k. Escorts will be technically competent and will ensure that visitors do nothing that might degrade or circumvent implemented security countermeasures or safeguards in WIN sites or equipment. (VII-5)
( ) ( ) NW

NOTE: WA--Waiver Authority. Waivers to this document may be approved by:

(S) - the local site DAA
(J) - Joint Staff
(NW) - nonwaiverable
Y = Yes; N = No.
Numbers in parentheses refer to paragraphs in this publication.

l. WIN users who are to be dismissed from a WIN access position under unfavorable circumstances will be denied all WIN access privileges immediately. (VII-7a)

( ) ( ) S

m. All WIN users who depart the WIN organization will be identified to the WASSO and WATASO by the commander of the user's organization. (VII-7a)

( ) ( ) S

CHAPTER VIII

PHYSICAL AND ENVIRONMENTAL SECURITY

17. Physical and Environmental Security

a. Physical security for multiuser host processor areas will satisfy the TOP SECRET open storage requirements of the DOD component concerned. (VIII-2)

( ) ( ) J

b. Physical security of WIN RNP/remote DATANET-8/Concentrator/LAN/terminal areas will be provided by either (VIII-3):

(1) Twenty-four hour manning by US TOP SECRET cleared personnel who are listed on the facility's access roster, (VIII-3a)

( ) ( ) J

(2) A Class A or B vault that meets the standards established by the head of the DOD component concerned, (VIII-3b)

( ) ( ) J

(3) A US Government controlled access area with motion detectors designed to detect unauthorized entry

NOTE: WA--Waiver Authority. Waivers to this document may be approved by:

(S) - the local site DAA
(J) - Joint Staff
(NW) - nonwaiverable
Y = Yes; N = No.
Numbers in parentheses refer to paragraphs in this publication.

which is deemed by the local responsible official to provide equivalent or better protection than Chapter VIII, subparagraphs a and b. (VIII-3c)

( ) ( ) J

c. Sites using securable containers will develop and indoctrinate users on operational procedures associated with their use. (VIII-4)

( ) ( ) J

(1) When in use, a physical control zone (controlled space) around the WIN workstation or terminal will be established to prevent access or viewing by unauthorized personnel. (VIII-4a)

( ) ( ) J

(2) TEMPEST countermeasures will be determined in accordance with NTISSI 7000 and implementing Service regulations. (VIII-4b)

( ) ( ) J

(3) If the area or room in which the securable container is used does not meet the conditions of paragraph 3 above, the encryption device (e.g., STU-III) used with the WIN workstation or terminal will be physically located inside the same securable container as the WIN workstation or terminal. In addition, no communication lines connecting the workstation or terminal to the encryption device will be allowed to run outside the securable container. (VIII-4c)

( ) ( ) J

NOTE: WA--Waiver Authority. Waivers to this document may be approved by:

(S) - the local site DAA
(J) - Joint Staff
(NW) - nonwaiverable
Y = Yes; N = No.
Numbers in parentheses refer to paragraphs in this publication.

(4) When not in use, cryptographic keying material will be safeguarded in accordance with published DOD COMSEC policies and procedures. (VIII-4d)

( ) ( ) J

d. To guard against sabotage or bugging, hardware to be connected to the WIN will be protected at the TOP SECRET level. This hardware will be protected by one of the following methods (VIII-5):

(1) Storing in a TOP SECRET area. (VIII-5a)

( ) ( ) J

(2) If TOP SECRET level protection is not achievable, WIN hardware must first be downgraded or all WIN data storage media inside the said hardware must be removed and stored in a TOP SECRET area. (VIII-5b)

( ) ( ) J

(a) The non-TOP SECRET area in which the equipment is located must be lockable and must not provide any opportunity to allow reconnection to the WIN without the WIN multiuser host intervention. (VIII-5b(1))

( ) ( ) J

(b) For added indication of tampering or bugging, NSA approved tamper-indicative seals may be used at the site DAA's discretion. If used, the site must develop local procedures for using and tracking for the life-cycle of the seals. (VIII-5b(2))

( ) ( ) S

NOTE: WA--Waiver Authority. Waivers to this document may be approved by:

(S) - the local site DAA
(J) - Joint Staff
(NW) - nonwaiverable
Y = Yes; N = No.
Numbers in parentheses refer to paragraphs in this publication.

(c) If, for any reason, the said seal has been removed or appears to have been tampered with, it must be assumed that the WIN hardware has been tampered with or bugged. A TSCM inspection of this WIN hardware must be performed before reconnection to the WIN. (VIII-5b(3))
( ) ( ) J

e. Utilities supporting WIN multiuser hosts are suitably protected. (VIII-6)
( ) ( ) S

CHAPTER IX

SOFTWARE SECURITY

18. Introduction and General Provisions

a. Introduction

(1) WIN software must have configuration management controls and will be approved through SDN process in accordance with Joint Pub 6-03.11. (IX-1a)
( ) ( ) J

(2) User, operator, and programmer documentation will include a description and explanation of software security features to allow for their effective use. (IX-1d)
( ) ( ) J

(3) Security software features, if any, will be part of IST. (IX-1e)
( ) ( ) J

NOTE: WA--Waiver Authority. Waivers to this document may be approved by:

(S) - the local site DAA
(J) - Joint Staff
(NW) - nonwaiverable
Y = Yes; N = No.
Numbers in parentheses refer to paragraphs in this publication.

b. Firmware

(1) Firmware will not be modified by WIN users without WASSO approval. (IX-2)

( ) ( ) J

(2) Field engineers will notify the WASSO when making a firmware change to other than T&DE. (IX-2b)

( ) ( ) S

c. Intelligent Terminal (Workstation) Software

(1) Joint, Service, or site developed software is developed by Government or contractor personnel and controlled in accordance with configuration management policy set forth in Joint Pub 6-03.11 as well as applicable Service and Defense agency regulations. (IX-3a)

( ) ( ) J

(2) The use of public domain software on the WIN requires SDN approval. (IX-3c)

( ) ( ) J

d. Protection of Software

(1) Software will be classified at the highest level of information or aggregation of information that can be derived from the software. (IX-4a)

( ) ( ) J

(2) Trusted software will be protected at the highest level of information it processes and placed under configuration control by

NOTE: WA--Waiver Authority. Waivers to this document may be approved by:

(S) - the local site DAA
(J) - Joint Staff
(NW) - nonwaiverable
Y = Yes; N = No.
Numbers in parentheses refer to paragraphs in this publication.

security personnel to ensure its trustworthiness. (IX-4b)
( ) ( ) J

(3) Government and contractor personnel who develop, modify, or maintain applications software must possess at least a US SECRET clearance. COTS software is exempt from this requirement unless it is modified for WIN usage. (IX-4c)
( ) ( ) J

e. Software Releases. Each multiuser host WASSO will verify the authenticity of software received by comparing the registry or shipment number of the software package with that contained in the message from the originating DDA and return the enclosed "shipment received" card to the DDA. If, after 15 days from the forwarding date, the site has not received the expected software shipment, it will advise the DDA through message so that the DDA may initiate tracer action. Each site will notify the DDA upon implementation of the new software. (IX-5c)
( ) ( ) J

f. All COTS will be screened for malicious software before installation on WIN computing equipment in accordance with Chapter XIX of this publication. (IX-5d)
( ) ( ) J

NOTE: WA--Waiver Authority. Waivers to this document may be approved by:

(S) - the local site DAA
(J) - Joint Staff
(NW) - nonwaiverable
Y = Yes; N = No.
Numbers in parentheses refer to paragraphs in this publication.

CHAPTER X

WIN SITE OPERATING SYSTEM SOFTWARE SECURITY

19. Operating System Software

a. Before implementing any new system release, the WIN site will verify that the system meets the requirements of Chapter X of this publication. (X-1)
( ) ( ) J

b. The WASSO will maintain a site log of all verified system changes or site-unique patches. All modifications to the operating system will be kept under close control and cross-checked by two appropriately cleared system programmers. (X-2)
( ) ( ) J

c. A master copy of the system start-up file should be maintained in a secure location of the WASSO. The start-up procedures must be described in the site SOP manual to provide a known processing environment. The WASSO staff will authenticate system patches by random checks of the patch section in the system start-up file. (X-2a)
( ) ( ) S

d. The WASSO will develop a method to control access to system tapes or disks. All unauthorized requests for system tapes or disks will be reported to the WASSO. (X-2b)
( ) ( ) S

e. Site unique patches that affect operation of the WIN require prior approval of the WIN DAA through an SDN. (X-3b)
( ) ( ) J

NOTE: WA--Waiver Authority. Waivers to this document may be approved by:

(S) - the local site DAA
(J) - Joint Staff
(NW) - nonwaiverable
Y = Yes; N = No.
Numbers in parentheses refer to paragraphs in this publication.

CHAPTER XI

APPLICATIONS SOFTWARE SECURITY FOR WIN SITES

20. Applications Software

a. Development Site-Unique Applications Software

(1) Security specifications for each new site-unique applications release will be developed and coordinated with the user, the computer installation manager, and the WASSM or WASSO before approval of the specifications. (XI-3a)

( ) ( ) S

(2) Design reviews will be conducted by the site to ascertain that the proposed design meets the approved security specifications. The results of the design review should be fully documented and maintained as official records of the site. (XI-3c)

( ) ( ) S

(3) System tests of each new application release will be conducted to demonstrate that the system meets the approved security specifications and complies with existing security policy. (XI-3d)

( ) ( ) S

b. Site modification of WIN standard COTS applications software must be approved by SDN in accordance with Joint Pub 6-03.11. (XI-4a)

( ) ( ) J

c. Use of site-unique COTS applications software in the WIN must be approved by

NOTE: WA--Waiver Authority. Waivers to this document may be approved by:

(S) - the local site DAA
(J) - Joint Staff
(NW) - nonwaiverable
Y = Yes; N = No.
Numbers in parentheses refer to paragraphs in this publication.

SDN in accordance with Joint Pub 6-03.11. (XI-4b(1))
( ) ( ) J

d. Site modification of site-unique COTS applications software used on the WIN must be approved in accordance with Joint Pub 6-03.11. (XI-4b(2))
( ) ( ) J

e. Use of public domain software and Shareware is prohibited unless the source code has been approved by the WIN DAA through an SDN in accordance with Joint Pub 6-03.11. (XI-5)
( ) ( ) J

CHAPTER XII

SYSTEM RESOURCE ACCESS AND CONTROL

21. Resource Access and Control

a. Passwords as User Authenticators

(1) The WASSO is responsible for generating and distributing the initial multiuser host SECRET logon Passwords for each USERID. (XII-2b)
( ) ( ) S

(2) Entry of WIN password on a terminal device will be protected from disclosure to anyone observing the entry process. (XII-2b(1))
( ) ( ) S

(3) The number of password entry attempts will be limited to no more than two successive tries. (XII-2b(2)
( ) ( ) S

NOTE: WA--Waiver Authority. Waivers to this document may be approved by:

(S) - the local site DAA
(J) - Joint Staff
(NW) - nonwaiverable
Y = Yes; N = No.
Numbers in parentheses refer to paragraphs in this publication.

(4) WIN users responsibilities (XII-2b(3)):

(a) Ensure no password disclosure.

( ) ( ) J

(b) Ensure no password loss.

( ) ( ) J

(5) Logon password will not be stored in ADP files by anyone other than the WASSO and WATASO. (XII-2b(4))

( ) ( ) J

(6) Changes. Passwords will be deleted or replaced under any of the following conditions (XII-2b(5)):

(a) Whenever an individual's access is withdrawn for any reason. (XII-2b(5)(a))

( ) ( ) J

(b) Whenever a password or record of a password has been or is suspected of having been compromised, immediate notification must be given to the WASSO and WATASO for password replacement and any further appropriate investigative action. (XII-2b(5)(b))

( ) ( ) J

(c) At least semiannually. (XII-2b(5)(c))

( ) ( ) J

NOTE: WA--Waiver Authority. Waivers to this document may be approved by:

(S) - the local site DAA
(J) - Joint Staff
(NW) - nonwaiverable
Y = Yes; N = No.
Numbers in parentheses refer to paragraphs in this publication.

(7) For LANs, the LAN Security Manager is responsible for issuing the initial LAN password to users of the LAN. (XII-2b(6))

( ) ( ) J

(8) For workstations with terminal logon password features, the WATASO or workstation administrator is responsible for issuing the initial workstation passwords to users of that WIN workstation. (XII-2b(7))

( ) ( ) J

b. Group USERIDs

(1) A Group Team Chief will be designated in writing. (XII-3b(1))

( ) ( ) J

(2) Group Team Chiefs will maintain a manual log of all group member's WIN access and it will be retained for 2 years for audit purposes. (XII-3b(2))

( ) ( ) J

(3) All team members will possess an interim or final US TOP SECRET clearance. Foreign nationals will not be allowed to be a team member of a group using a group USERID. (XII-3b(3))

( ) ( ) J

(4) Whenever a group member departs the group, and that member knew the Group USERID password, the WASSO will be notified. The password will be changed by the team chief. (XII-3b(4))

( ) ( ) J

(5) Group USERIDs approved by the local DAA will not be given WIN

NOTE: WA--Waiver Authority. Waivers to this document may be approved by:

(S) - the local site DAA
(J) - Joint Staff
(NW) - nonwaiverable
Y = Yes; N = No.
Numbers in parentheses refer to paragraphs in this publication.

access permissions without approval of the WIND. (XII-3c)
( ) ( ) J

(6) If a group USERID requires WIN access permissions, the DAA will approve the group USERID and forward the access request to the WIND for network access approval. (XII-3d)
( ) ( ) J

(7) Annually, site WSCs will notify the WIND and other WIN site WSCs/WASSOs if continued use of the group USERID is necessary. (XII-3e)
( ) ( ) J

(8) A project USERID or account will not be allowed to logon to the WIN. (XII-3g)
( ) ( ) J

c. Revalidation of Individual USERIDs

(1) Multiuser host access revalidation will be performed semiannually by the WSC. (XII-3h(1))
( ) ( ) J

(2) Network access revalidation will be performed semiannually by each multiuser host site. (XII-3h(2))
( ) ( ) J

d. Access Permissions in the File System

(1) Positive controls must be used to control access to all classified or special category objects (catalogs, directories, files, etc.). General access will not be given to any classified file or to any file structure that contains a classified

NOTE: WA--Waiver Authority. Waivers to this document may be approved by:

(S) - the local site DAA
(J) - Joint Staff
(NW) - nonwaiverable
Y = Yes; N = No.
Numbers in parentheses refer to paragraphs in this publication.

or special category file. Personnel who depart or no longer need access to a file should have their access permissions deleted as soon as possible by project or file OPR. (XII-4c(1))

( ) ( ) J

(2) WIN user should be provided with the proper procedures for requesting access to WIN files at local and remote sites. The file OPR of the multiuser host where the file resides verifies the need-to-know of the requesting WIN user. (XII-4c(2))

( ) ( ) S

e. Permission to Functions. Positive controls will be used to control access to all functions that can affect the security or integrity of the WIN. Access of this type will be approved by the WASSO and will be kept to the absolute minimum number of personnel. (XII-4d)

( ) ( ) J

f. Audit Requirements

(1) The manual or automated audit trail will be able to document, at a minimum, the seven event types defined in Chapter XII, subparagraph 5b of this document. (XII-5b)

( ) ( ) J

(2) The WASSO will identify and recommend appropriate actions on security-related events in the audit trail. System surveillance will be under the control of the WASSO. Audit trails will be reviewed at least weekly and follow-up action taken on all discrepancies.

NOTE: WA--Waiver Authority. Waivers to this document may be approved by:

(S) - the local site DAA
(J) - Joint Staff
(NW) - nonwaiverable
Y = Yes; N = No.
Numbers in parentheses refer to paragraphs in this publication.

Suspected security incidents will be reported to the local site WASSO for action. The NOC will be notified of any serious actions planned or taken as a result of the incident investigation. (XII-5d)

( ) ( ) J

(3) Audit data defined in the machine specific STP will be reviewed periodically. Incidents will be reported as required in Chapter I. (XII-5e(1))

( ) ( ) S

(4) Network audit reports will be available for review by the WASSO for each period of WIN operations. The WASSO will be informed of any suspect activities. The NOC will be informed of any suspected security incidents related to network operations. (XII-5e(2))

( ) ( ) J

g. System Profile and File Structure Management. The WASSO should analyze the system master profile and file structure on a daily basis for any discrepancies. (XII-6)

( ) ( ) S

NOTE: WA--Waiver Authority. Waivers to this document may be approved by:

(S) - the local site DAA
(J) - Joint Staff
(NW) - nonwaiverable
Y = Yes; N = No.
Numbers in parentheses refer to paragraphs in this publication.

h. Privileged States or Functions

(1) Jobs or processes that require privileged states or functions will only be authorized by the multiuser host DAA or his designated representative. A listing of those jobs, processes, or users will be maintained in the site for the operators to verify approval prior to granting privity. (XII-7a)

( ) ( ) J

(2) Standard or Service unique WIN application systems will not be developed with a privileged state requirement unless prior approval of network DAA has been received. (XII-7b)

( ) ( ) J

i. Terminal Time-Out. Terminal will be timed out after 10 minutes if it has not processed any input or output transaction. (XII-9)

( ) ( ) S

j. Periods Processing. Between periods processing, memory will be purged using DISA-approved software, and that purge will be verified. The system packs and removable media, classified at the level appropriate for the period, will be used at system startup. The peripheral subsystems will be initialized according to site procedures. (XII-10b)

( ) ( ) J

NOTE: WA--Waiver Authority. Waivers to this document may be approved by:

(S) - the local site DAA
(J) - Joint Staff
(NW) - nonwaiverable
Y = Yes; N = No.
Numbers in parentheses refer to paragraphs in this publication.

CHAPTER XIII

HARDWARE SECURITY

22. Hardware Security

a. Hardware to be used in the WIN will be approved through the SDN process, in accordance with Joint Pub 6-03.11, and will have configuration management controls to protect it against unauthorized alteration. (XIII-1)

( ) ( ) J

b. Hardware will be declassified at the end of each day's processing unless it is located in a storage area approved for TOP SECRET open storage. If the hardware becomes inoperable, it will be protected at the TOP SECRET level until destroyed and a destruction certificate is initiated. (XIII-2)

( ) ( ) J

c. Hardware containing nonremovable magnetic media will be declassified at the end of each day or stored in a TOP SECRET open storage area. (XIII-3a)

( ) ( ) J

d. Hardware containing nonremovable magnetic media will be declassified before turn-in for maintenance. (XIII-3b)

( ) ( ) J

e. Hardware that is to be decommissioned and no longer operated on the WIN will have its nonremovable magnetic media declassified or its removable magnetic media removed and stored according to its classification. (XIII-3c)

( ) ( ) J

NOTE: WA--Waiver Authority. Waivers to this document may be approved by:

(S) - the local site DAA
(J) - Joint Staff
(NW) - nonwaiverable
Y = Yes; N = No.
Numbers in parentheses refer to paragraphs in this publication.

f. Memory component spare parts (such as memory boards) for WIN hardware must be protected at the TOP SECRET level when they are on-site and identified as WIN hardware spare parts. (XIII-5)

( ) ( ) J

g. WIN hardware end items will not be procured from foreign vendors unless previously approved by the Joint Staff. (XIII-6a)

( ) ( ) J

h. ROMs, PROMs, and other varieties of precoded memory chips identified for use on the WIN will not be procured from a foreign vendor without Joint Staff approval. (XIII-6b)

( ) ( ) J

i. There will be no modifications to WIN hardware without prior notification of the WASSO. Generally, there will be no modifications to the hardware unless they are (XIII-7):

( ) ( ) J

(1) Part of a maintenance contract. (XIII-7a)

( ) ( ) J

(2) Site unique and preapproved by an SDN in accordance with Joint Pub 6-03.11. (XIII-7b)

( ) ( ) J

j. Methods provided in NCSC-TG-008 will be used for distribution of all hardware, firmware, and software. (XIII-8b)

( ) ( ) J

NOTE: WA--Waiver Authority. Waivers to this document may be approved by:

(S) - the local site DAA
(J) - Joint Staff
(NW) - nonwaiverable
Y = Yes; N = No.
Numbers in parentheses refer to paragraphs in this publication.

CHAPTER XIV

EMANATIONS SECURITY

23. Emanations Security

a. WIN users will comply with the measures to control compromising emanations provided under DOD Directive C-5200.19, "Control of Compromising Emanations." (XIV-1a)

( ) ( ) J

b. The countermeasures to be implemented for WIN sites will be determined in accordance with NTISSI 7000. On-site vulnerability analysis, tests, and inspection or other appropriate verification procedures will be used to demonstrate TEMPEST countermeasures acceptability. The WIN multiuser host DAA may elect to accept a higher risk by not implementing countermeasures to the level determined in accordance with NTISSI 7000. If this decision is made, it will be documented with justification in the site Risk Analysis report. (XIV-1b)

( ) ( ) J

c. Devices that have no known TEMPEST profile will be tested before being installed on site to determine the CS required, minimum essential countermeasures required, or possible equipment modification. If the equipment model has not been previously tested (i.e., has no known TEMPEST profile), it may be tested by sending the equipment to the appropriate Service agency or, preferably, by having an on-site survey. (XIV-2b)

( ) ( ) J

NOTE: WA--Waiver Authority. Waivers to this document may be approved by:

(S) - the local site DAA
(J) - Joint Staff
(NW) - nonwaiverable
Y = Yes; N = No.
Numbers in parentheses refer to paragraphs in this publication.

d. When repairs or changes are made to meet prescribed emanation requirements, every effort should be made to use exact replacement components or components known to possess equivalent or superior TEMPEST characteristic. If this cannot be done, a new TEMPEST survey will be accomplished. (XIV-3)

( ) ( ) J

CHAPTER XV

COMMUNICATIONS SECURITY

24. COMSEC

a. All communication links among WIN sites will meet the security requirements for the transmission of TOP SECRET data, as well as all restrictive categories of material processed by the attached devices. (XV-2)

( ) ( ) J

b. Use of dial-up devices in the WIN for data transmission requires the dial-up devices be physically located in a TOP SECRET area and afforded the same protection as the WIN components. (XV-3)

( ) ( ) J

c. Connecting secure dial-up devices to a WIN multiuser host requires:

(1) Prior WIN DAA approval. (XV-3)

( ) ( ) J

(2) Thorough evaluation by the multiuser host DAA of the risks involved and, in particular, the denial of service potential. (XV-3a)

( ) ( ) J

NOTE: WA--Waiver Authority. Waivers to this document may be approved by:

(S) - the local site DAA
(J) - Joint Staff
(NW) - nonwaiverable
Y = Yes; N = No.
Numbers in parentheses refer to paragraphs in this publication.

(3) All communications connections must be in compliance with NACSIM 5203, "Guidelines for Facility Design and Red/Black Installation." (XV-4 & XV-3b)
( ) ( ) J

(4) When the device, crypto, and associated modem are connected, physical security must be provided in accordance with the requirements established in Chapter VIII. (XV-3c)
( ) ( ) J

(5) Supplementary control must be established to audit the identity of the device making the connection. (XV-3d)
( ) ( ) J

(6) A list of all approved dial-up devices must be maintained at the hosting WIN site. (XV-3e)
( ) ( ) J

(7) All terminal access attempts must be audited. (XV-3f)
( ) ( ) J

(8) Telephone numbers and devices with call forwarding capability must not be used. (XV-3g)
( ) ( ) J

d. Secure Telephone Unit III (STU-III):

(1) STU-III users will comply with the operational security doctrine of NTISSI No. 3013. (XV-4)
( ) ( ) J

(2) Use of the STU-III within an area that meets the physical security requirements of Chapter VIII of this

NOTE: WA--Waiver Authority. Waivers to this document may be approved by:

(S) - the local site DAA
(J) - Joint Staff
(NW) - nonwaiverable
Y = Yes; N = No.
Numbers in parentheses refer to paragraphs in this publication.

publication will comply with the following conditions:

(a) The Type 1 STU-III will be equipped with SACS. (XV-4a(1))

( ) ( ) J

(b) Operating the STU-III in the Attended Mode is acceptable under the following conditions:

1. The STU-III will be physically located in the same TOP SECRET control area as the WIN terminal or workstation to which it is attached. (XV-4a(2)(a))

( ) ( ) J

2. The STU-III will be programmed to accept only TOP SECRET connections. (XV-4a(2)(b))

( ) ( ) J

3 The STU-III will not be allowed to be connected to another STU-III for more than 24 hours in a single session. After 24 hours, a new session can be initiated if necessary. (XV-4a(2)(c))

( ) ( ) J

(c) When operated in the unattended mode the requirements of para XV-4a(2)(a), (b), and (c) will be met and DAO codes that specify department, agencies, or organizations will be used. (XV-4a(3))

( ) ( ) J

NOTE: WA--Waiver Authority. Waivers to this document may be approved by:

(S) - the local site DAA
(J) - Joint Staff
(NW) - nonwaiverable
Y = Yes; N = No.
Numbers in parentheses refer to paragraphs in this publication.

(3) When used outside a TOP SECRET control zone, a securable container will be used such as the Secure Desk (KWS-5203) that meets the physical security requirements of Chapter VIII of this publication. (XV-4b)

( ) ( ) J

(4) Use of the STU-III in these securable containers is authorized subject to the following conditions:

(a) The conditions of paragraph XV-4a are observed except that the STU-III will not be operated in the unattended mode. (XV-4b(1))

( ) ( ) J

(b) The securable container has been authorized for use by the multiuser host DAA. (XV-4b(2))

( ) ( ) J

(c) Operation of the WIN terminal in the securable container conforms to the conditions specified in Chapter VIII of this publication. (XV-4b(3))

( ) ( ) J

(d) While in use, the STU-III will be located inside the securable container. This ensures that no communication lines between the WIN terminal and the STU-III are exposed and subject to a threat attack. (XV-4b(4))

( ) ( ) J

NOTE: WA--Waiver Authority. Waivers to this document may be approved by:

(S) - the local site DAA
(J) - Joint Staff
(NW) - nonwaiverable
Y = Yes; N = No.
Numbers in parentheses refer to paragraphs in this publication.

(5) Use of the STU-III on the DSN will comply with CJCS MOP 8. (XV-4c)
( ) ( ) J

(6) WIN connections to AUTODIN will ensure that the security protection of AUTODIN is not diminished. Connection to AUTODIN requires that the AUTODIN connection be accredited as described in Chapter V. (XV-5)
( ) ( ) J

CHAPTER XVI

INFORMATION SECURITY

25. Security of ADP Output Products and Storage Media

a. WIN output products that contain TOP SECRET data are accounted for in accordance with DOD 5200.1-R. (XVI-2b)
( ) ( ) NW

b. Users and customers will sign for all output. A log identifying the product and the user or customer may be used for this purpose. The log should be retained for a period of 1 year. (XVI-2b)
( ) ( ) J

c. Formal accountability of TOP SECRET output products is the user's or customer's responsibility. (XVI-2b)
( ) ( ) S

d. All WIN output products will be marked with the proper classification of the data present. (XVI-3)
( ) ( ) J

e. All printed paper products will be marked with the user's intended security

NOTE: WA--Waiver Authority. Waivers to this document may be approved by:

(S) - the local site DAA
(J) - Joint Staff
(NW) - nonwaiverable
Y = Yes; N = No.
Numbers in parentheses refer to paragraphs in this publication.

classification on the top and bottom of each page. (XVI-3a)
( ) ( ) J

f. Microfilm and microfiche will be conspicuously marked (i.e., eye readable) with the highest security classification of the data contained therein, date of creation, and unique identifier. (XVI-3b)
( ) ( ) J

g. Output of CRT screen printers will have classification markings on the top and bottom of each page. The marking can be produced by software or manually. (XVI-3c)
( ) ( ) J

h. WIN magnetic media must be formally accounted for as TOP SECRET whenever it leaves the confines of the WIN TOP SECRET area unless it has been downgraded to a lower classification. (XVI-4b)
( ) ( ) NW

i. All removable ADP storage media used on hardware attached to the WIN will be externally marked TOP SECRET until declassified or downgraded. This marking will be written and color-coded orange. The use of color-coded media or labels is required. Exceptions are listed in paragraph XVI-5b. (XVI-5a)
( ) ( ) J

j. Permanently mounted ADP storage media will be conspicuously marked TOP SECRET on the outside of the hardware in which it resides. (XVI-5a(3))
( ) ( ) J

k. Clearing of magnetic media will be used when data stored on the media is no

NOTE: WA--Waiver Authority. Waivers to this document may be approved by:

(S) - the local site DAA
(J) - Joint Staff
(NW) - nonwaiverable
Y = Yes; N = No.
Numbers in parentheses refer to paragraphs in this publication.

longer required by the data owner, but the media will continue to be used for the WIN. Clearing will be accomplished with overwrite software that has been approved by the WASO. (XVI-6b(1))
( ) ( ) J

l. Declassification will be used when the media is to be decommissioned or released into a less than TOP SECRET and nongovernment controlled environment. (XVI-6b(2)(a))
( ) ( ) J

m. A Declassification Audit Report will be submitted to the WASSO or WASSM, which will be retained for a period of 1 year. (XVI-6b(2)(b))
( ) ( ) J

n. Transferring WIN data to media for use on a less than TOP SECRET AIS meets all requirements of paragraph XVI-6b(3). (XVI-6b(3))
( ) ( ) J

o. Destruction is currently the only approved method of declassifying non-magnetic storage media. As other non-magnetic permanent storage media become available, requests to declassify these media by means other than destruction will be submitted to the WASO for approval. (XVI-7)
( ) ( ) J

p. Volatile semiconductor memory is declassified by removal of all power (external and battery)for a period not less than 5 minutes. (XVI-8a)
( ) ( ) J

q. Nonvolatile semiconductor memory devices such as ROM, EPROM, EEPROM, etc.,

NOTE: WA--Waiver Authority. Waivers to this document may be approved by:

(S) - the local site DAA
(J) - Joint Staff
(NW) - nonwaiverable
Y = Yes; N = No.
Numbers in parentheses refer to paragraphs in this publication.

will be declassified either by overwrite or destruction as applicable. (XVI-8b)
( ) ( ) J

r. T&DE must be declassified or downgraded to UNCLASSIFIED before being removed from the WIN site. (XVI-9)
( ) ( ) J

CHAPTER XVII

WORKSTATION SECURITY

26. Approval to Connect. Only workstations approved by SDN in accordance with Joint Pub 6-03.11 will be connected to the WIN or to other hardware connected to the WIN. (XVII-2)
( ) ( ) J

27. Resource Access and Control

a. Need-to-know separation of data will be maintained on WIN microcomputer workstations. (XVII-3a(2))
( ) ( ) J

b. Workstation-to-workstation connectivity is authorized, provided (XVII-3b):

(1) Workstations maintain the same level of identification, authentication, access control and audit as the WIN multiuser host. (XVII-3b(1))
( ) ( ) J

(2) Privileged USERID passwords are unique for each system administrator. (XVII-3b(2))
( ) ( ) J

NOTE: WA--Waiver Authority. Waivers to this document may be approved by:

(S) - the local site DAA
(J) - Joint Staff
(NW) - nonwaiverable
Y = Yes; N = No.
Numbers in parentheses refer to paragraphs in this publication.

(3) Workstation administrators ensure that users do not inadvertently gain unauthorized privilege through remote access to another workstation. (XVII-3b(3))
( ) ( ) J

28. Physical Security. The provisions of Chapter VIII, especially paragraphs VIII-3 and VIII-5, apply to WIN terminal areas, and thus, apply to WIN workstations. (XVII-4a)
( ) ( ) J

29. Workstation Lockout. To prevent bugging of the hardware or terminal area, escorts are required for facility maintenance personnel, even when workstations are locked out. (XVII-4b)
( ) ( ) J

30. Privately owned hardware and software (i.e., not procured and owned by the US Government) will not be used on the WIN multiuser host or its workstations. (XVII-5)
( ) ( ) J

31. If workstations are required to be disconnected from the WIN and serve some other function (stand alone or connected to some other network), the following minimum requirements must first be met (XVII-6):

a. The workstation will be physically disconnected from the WIN. (XVII-6a)
( ) ( ) J

b. Workstation magnetic media will be removed.

NOTE: If the workstation has nonremovable magnetic media, it will be declassified by overwriting. (XVII-6b)
( ) ( ) J

NOTE: WA--Waiver Authority. Waivers to this document may be approved by:

(S) - the local site DAA
(J) - Joint Staff
(NW) - nonwaiverable
Y = Yes; N = No.
Numbers in parentheses refer to paragraphs in this publication.

c. Any workstation internal memory will be declassified. (XVII-6c)
( ) ( ) J

d. The workstation will continue to be physically protected at a TOP SECRET level. If the workstation must be used outside the WIN site, paragraph 5, Chapter VIII, applies. (XVII-6d)
( ) ( ) J

e. Separate operating system software and utilities will be maintained for processing of information at a level less than TOP SECRET. (XVII-6e)
( ) ( ) J

f. Written periods processing procedures will be maintained in each WIN terminal area. (XVII-6f)
( ) ( ) S

32. Security Administration. Multiuser intelligent workstations will have a security administrator assigned to perform security administration for the workstations. (XVII-7)
( ) ( ) J

33. Audit. Audit data will be selectively acquired based on auditing needs determined by the workstation Security Administrator. At a minimum, the following events will be audited (XVII-8a):
( ) ( ) J

a. Startup and shutdown.

b. Logon and logoff.

c. Object create, modify, or delete.

NOTE: WA--Waiver Authority. Waivers to this document may be approved by:

(S) - the local site DAA
(J) - Joint Staff
(NW) - nonwaiverable
Y = Yes; N = No.
Numbers in parentheses refer to paragraphs in this publication.

34. Security of the Audit Mechanism. The audit mechanism will be secure from user or unauthorized manipulation. (XVII-8d)
( ) ( ) J

CHAPTER XVIII

WIN SITE CONTINGENCY PLANNING

35. Contingency Planning. WIN sites will prepare plans to provide for the continuity of operations under varying conditions. (XVIII-1a)
( ) ( ) J

CHAPTER XIX

MALICIOUS SOFTWARE

36. Positive actions will be taken by management, technical support personnel, and users to protect the WIN from malicious software. In particular, the following actions are required. (XIX-4)

a. Education. Personnel associated with the WIN will familiarize themselves with materials that discuss the nature, variety, mechanisms, and effects of malicious software. (XIX-4a)
( ) ( ) J

b. Training. Personnel associated with the WIN will be introduced initially to malicious software as part of their introductory training. Thereafter, on an annual basis, additional training will be received, particularly on the latest threat developments. (XIX-4b)
( ) ( ) J

c. Prevention Program. Site management will procure COTS antiviral software that

NOTE: WA--Waiver Authority. Waivers to this document may be approved by:

(S) - the local site DAA
(J) - Joint Staff
(NW) - nonwaiverable
Y = Yes; N = No.
Numbers in parentheses refer to paragraphs in this publication.

is designed to detect, and correct in some cases, malicious software. (XIX-4c)
( ) ( ) J

d. Sites will institute procedures to ensure that a scan is made of all WIN microcomputers for malicious software at the following times (XIX-4c):
( ) ( ) J

(1) Prior to their first connection to the WIN. (XIX-4c(1))
( ) ( ) J

(2) On at least a monthly basis. (XIX-4c(2))
( ) ( ) J

(3) When a new software product or product upgrade is installed. (XIX-4c(3))
( ) ( ) J

37. Responsibilities

a. DAAs will ensure that workstations connected to their multiuser host have current antiviral software install and operating. (XIX-5a(5))
( ) ( ) J

b. WASSOs will:

(1) Ensure that new users are adequately briefed on malicious software as part of their initial training. (XIX-5c(1))
( ) ( ) J

(2) Receive current threat information as part of their required annual training. (XIX-5c(2))
( ) ( ) J

NOTE: WA--Waiver Authority. Waivers to this document may be approved by:

(S) - the local site DAA
(J) - Joint Staff
(NW) - nonwaiverable
Y = Yes; N = No.
Numbers in parentheses refer to paragraphs in this publication.

(3) Ensure that antiviral software is distributed to WATASOs for installation. (XIX-5c(3))
( ) ( ) J

(4) Immediately inform the DISA of a confirmed malicious software attack. Also, inform the site DAA, WSC, and the WASO. (XIX-5c(4))
( ) ( ) J

(5) Prepare a report (see paragraph 6 of this chapter) on the results from the investigation resulting from a malicious software attack. (XIX-5c(5))
( ) ( ) J

(6) Ensure that the malicious software attack report is forwarded to the WASO and DISA. (XIX-5c(6))
( ) ( ) J

c. WATASOs will:

(1) Ensure that workstation or terminal users have an adequate understanding of malicious software and know to notify the WATASO of a suspected attack. (XIX-5d(1))
( ) ( ) J

(2) Immediately isolate a workstation from the WIN if an attack is suspected and notify the WASSO. (XIX-5d(2))
( ) ( ) J

(3) Conduct an investigation if a malicious software attack occurs. (XIX-5d(3))
( ) ( ) J

NOTE: WA--Waiver Authority. Waivers to this document may be approved by:

(S) - the local site DAA
(J) - Joint Staff
(NW) - nonwaiverable
Y = Yes; N = No.
Numbers in parentheses refer to paragraphs in this publication.

d. LAN Security Managers will:

(1) Ensure that workstation or terminal users have an adequate understanding of malicious software and know to notify the WATASO of a suspected attack. (XIX-5e(1))
( ) ( ) J

(2) Immediately isolate a workstation from the LAN if an attack is suspected and notify the WASSO. (XIX-5e(2))
( ) ( ) J

(3) Conduct an investigation if a malicious software attack occurs. (XIX-5e(3)
( ) ( ) J

(4) Scan all software for malicious code before installing it on the LAN. (XIX-5e(4))
( ) ( ) J

38. Reporting. Upon confirming that a malicious software attack has occurred, the WATASO, under the guidance of the WASSO, will conduct an investigation leading to a Malicious Software Attack Report. (XIX-6)
( ) ( ) J

NOTE: WA--Waiver Authority. Waivers to this document may be approved by:

(S) - the local site DAA
(J) - Joint Staff
(NW) - nonwaiverable
Y = Yes; N = No.
Numbers in parentheses refer to paragraphs in this publication.

APPENDIX H

EXCERPT FROM ESPIONAGE ACT
(Title 18, United States Code)

Section 793. Gathering, transmitting, or losing Defense information

(a) Whoever, for the purpose of obtaining information respecting the national defense with intent or reason to believe that the information is to be used to the injury of the United States, or to the advantage of any foreign nation, goes upon, enters, flies over, or otherwise obtains information concerning any vessel, aircraft, work of defense, navy battery, torpedo station, dockyard, canal, railroad, arsenal, camp, factory, mine, telephone, wireless, or signal, station, building, office, research laboratory or station or other place connected with the national defense owned or constructed, or in progress of construction by the United States or under the control of the United States, or the exclusive jurisdiction of the United States, or any place in which any vessel, aircraft, arms munitions, or other material or instruments for use in time of war are being made, prepared, repaired, stored, or are the subject of research or development, under any contract or agreement with the United States, or any department or agency thereof, or with any person on behalf of the United States, or any prohibited place so designated by the President by proclamation in time of war in case of national emergency in which anything for the use of the Army, Navy, or Air Force is being prepared or constructed or stored, information as to which prohibited place the President has determined would be prejudicial to the national defense; or

(b) Whoever, for the purpose aforesaid, and with like intent or reason to believe, copies, takes, makes, or obtains, or attempts to copy, take, make, or obtain, any sketch, photograph, photographic negative, blueprint, plan, map, model, instrument, appliance, document, writing, or note of anything connected with the national defense; or

(c) Whoever, for the purposes of aforesaid, receives or obtains or agrees or attempts to receive or obtain from any person, or from any source whatever, any document, writing, code book, signal book, sketch, photograph, photographic negative, blueprint, plan, map, model, instrument, appliance, or note of anything connected with the national defense, knowing or having reason to believe, at the time he receives or obtains, or agrees or attempts to receive or obtain it, that is has been or

will be obtained, taken, made or disposed of by any person contrary to the provisions of this chapter; or

(d) Whoever, lawfully having possession of, access to, control over, or being entrusted with any document, writing, code book, signal book, sketch, photograph, photographic negative, blueprint, plan, map, model, instrument, appliance, or note relating to the national defense, or information relating to the national defense which information the possessor has reason to believe could be used to the injury of the United States or to the advantage of any foreign nation, willfully communicates, delivers, transmits or causes to be communicated, delivered, or transmitted or attempts to communicate, deliver, transmit the same to any person not entitled to receive it, or willfully retains the same and fails to deliver it on demand to the officer or employee of the United States entitled to receive it; or

(e) Whoever having unauthorized possession of, access to, or control over any document, writing, code book, signal book, sketch, photograph, photographic negative, blueprint, plan, map, model, instrument, appliance, or note relating to the national defense, or information relating to the national defense which information the possessor has reason to believe could be used to the injury of the United States or to the advantage of any foreign nation, willfully communicates, delivers, transmits or causes to be communicated, delivered, or transmitted or attempts to communicate, deliver, transmit or cause to be communicated, delivered, or transmitted the same to any person not entitled to receive it, or willfully retains the same and fails to deliver it on demand to the officer or employee of the United States entitled to receive it; or

(f) Whoever, being entrusted with or having lawful possession or control of any document, writing, code book, signal book, sketch, photograph, photographic negative, blueprint, plan, map, model, instrument, appliance, note, or information, relating to the national defense, (1) through gross negligence permits the same to be removed from its proper place of custody or delivered to anyone in violation of his trust, or to be lost, stolen, abstracted, or destroyed, or (2) having knowledge that the same has been illegally removed from its proper place of custody or delivered to anyone in violation of his trust, or lost, or stolen, abstracted, of destruction -- will be fined not more than $10,000 or imprisoned not more than 10 years, or both.

(g) If two or more persons conspire to violate any of the foregoing provisions of this section, and one or

more of such persons do any act to effect the object of conspiracy, each of the parties to such conspiracy will be subject to the punishment provided for the offense which is the object of such conspiracy, 25 June 1984. c.645, s.1, 62 Stat. 736, amended 23 September 1950, c. 1024, s.18 64 Stat.---

Section 794, Gathering or delivering defense information to aid foreign government

(a) Whoever, with intent or reason to believe that it is to be used to the injury of the United States or to the advantage of a foreign nation, communicates, delivers, or transmits, or attempts to communicate, deliver, or transmit, to any foreign government, or to any faction or party or military or naval force within a foreign country, whether recognized by the United States, or to any representative, officer, agent, employee, subject, or citizen thereof, either directly or indirectly, any document, writing, code book, signal book, sketch, photograph, photographic negative, blueprint, plan, map, model, note, instrument, or information relating to the national defense, will be punished by death or by imprisonment for any term of years or for life.

(b) Whoever, in time of war, with intent that the same will be communicated to enemy, collects, records, publishes, or communicates, or attempts to elicit any information with respect to the movement, numbers, description, condition, or disposition of any of the Armed Forces, ships, aircraft, or war materials of the United States, or with respect to the plans or conduct, or supposed plans or conduct, of any naval military operations, or with respect to any works or measures undertaken for connected with, or intended for the fortification or defense of any place, or any other information relating to the public defense, which might be useful to the enemy, will be punished by death or by imprisonment for any term of years or for life.

(c) If two or more persons conspire to violate this section, and one or more of such persons do any act to effect the object of conspiracy, each of the parties to such conspiracy will be subject of such conspiracy. As amended 3 September 1954, c. 1261, Title II, s. 201, 68 Stat. 1219.

(INTENTIONALLY BLANK)

APPENDIX J

FORMAT AND MINIMUM INFORMATION REQUIRED FOR WIN-AIS MOA

MEMORANDUM OF AGREEMENT
between

_____, DAA for the (Site name and location)

and

_____, DAA for the (AIS name and location)

In accordance with DOD Directive 5200.28, a Memorandum of Agreement (MOA) is established herein. The terms and conditions of this MOA are set forth as follows:

I. Purpose: State Requirement for Connection.

II. Description:

A. Name of AIS.

1. DAA Name and Billet Title.
2. Classification of Data.
3. Clearance Level of Users.
4. Stand-Alone TCSEC Class (e.g., C2).
5. Connected AISs.
a. AIS (Name).
b. AIS (Name).
6. Applicable Policy Document (e.g., Joint Pub 6-03.7).

B. Name of WIN Host.

1. DAA Name and Billet Title.
2. Classification of Data.
3. Clearance Level of Users.
4. Stand-Alone TCSEC Class (e.g., C2).
5. Connected AISs.
a. AIS (Name).
b. AIS (Name).
6. Applicable Policy Document (e.g., Joint Pub 6-03.7).

III. Interface Description:

IV. Security Requirements:

A. Calculated Risk Index (DODD 5200.28, Encl (4)).
B. Who Resolves Conflicts.
C. Safeguards Required.
D. Guard Specifications:
1. Description.
2. Name of POC.
3. Guard Documentation (Identify Documents with Dates).
a. Security Architecture.
b. Concept of Operations.
c. Test Document.
d. Operator's Manual.
e. User's Manual.

IV. Responsibilities:

A. Guard Operations and Maintenance.
B. Security Administration.

V. Life-cycle Management:

A. Change Protocol.
B. Maintenance of Documentation.

VI. COOP:

Signatures:

DAA for WWMCCS AIS

Name Billet

DAA for Connecting AIS

Name Billet

GLOSSARY

PART I - ABBREVIATIONS AND ACRONYMS

.NL.	not less than
ACL	access control list
ADP	automatic data processing
ADPE	automatic data processing equipment
ADPS	automatic data processing system
AFR	Air Force Regulation
AIG	address indicating group
AIS	Automated Information System
AMH	Automated Message Handler
AR	Army Regulation
ATC	Air Training Command
AUTODIN	Automatic Digital Network
AWASSO	Assistant WASSO
CINC	commander of a unified or specified command
CNWDI	Critical Nuclear Weapons Design Information
COMPUSEC	computer security
COMSEC	communications security
CONUS	continental United States
COOP	Continuity of Operations Plan
COSMIC	NATO Security Category
COTS	commercial-off-the-shelf
CPU	central processing unit
CRT	cathode ray tube
CS	controlled space
CSAM	Computer Security for Acquisition Managers
DAA	designated approving authority
DAO	Department/Agency/Organization
DDA	Designated Development Activity
DDN	Defense Data Network
DIAM	Defense Intelligence Agency Manual
DICO	Data Information Coordination Office
DISA	Defense Information Systems Agency
DISN	Defense Information Systems Network
DODD	Department of Defense directive
DPS	Data Processing System (used By HFSI, Inc.)
DSN	Defense Switched Network
DSNET2	Defense Secure Network 2
DISA	Defense Information Systems Agency
EEPROM	electronic erasable programmable read-only memory
EFTO	encrypt for transmission only
EMSEC	emanations security
EPROM	electronic programmable read-only memory
ETPL	Endorsed TEMPEST Products List
FOUO	For Official Use Only

GSA	General Services Administration
ID	indentification
IDHS	Intelligence Data Handling System
INFOSEC	information security
ISOO	Information Security Oversight Office
IST	Integrated System Test
JCAT	Joint Crisis Action Team
JDS	Joint Deployment System
JOPES	Joint Operations Planning And Execution System
JOPS	Joint Operations Planning System
LAN	local area network
MLS	multilevel security
MOA	memorandum of agreement
MOP	memorandum of policy
MOR	memorandum of record
MSECR	HIS 6000 Security Module
NACSEM	National COMSEC/EMSEC Information Memorandum
NACSI	National COMSEC Instruction
NACSIM	National COMSEC Information Memorandum
NATO	North Atlantic Treaty Organization
NCA	National Command Authorities
NCSC	National Computer Security Center
NMCC	National Military Command Center
NMCS	National Military Command System
NOC	Network Operations Center
NSA	National Security Agency
NTISS	National Telecommunications and Information Security
NTISSI	NTISS Instruction
NTISSP	NTISS Policy
NW	not waiverable
OCONUS	outside continental United States
OMB	Office of Management and Budget
OPR	office of primary responsibility
PCZ	Physical Control Zone
PDS	Protected Distribution System
PMO	Program Management Office
PROM	programmable read-only memory
PSN	Packet Switching Node
RA	Risk Analysis
RFP	request for proposal
RLP	Remote Line Printer
RNP	Remote Network Processor
ROM	read-only memory

SACS	STU Access Control System
SAPI	Special Access Program for Intelligence
SCC	Security Classification Code
SCI	Sensitive Compartmented Information
SCP	System Change Proposal
SDN	System Development Notification
SIOP-ESI	Single Integrated Operational Plan--Extremely Sensitive Information
SMC	System Master Catalog
SOP	standard operating procedure
SOW	statement of work
SRB	Software Release Bulletin
ST&E	Security Test And Evaluation
STP	Security Technical Procedure
STU-III	Secure Telephone Unit III
T&DE	test & diagnostic equipment
TCSEC	Trusted Computer System Evaluation Criteria
TI	Technical Instruction For WSCs
TPFDD	Time-Phased Forced Deployment Data
TSCM	technical surveillance countermeasures
TSCO	TOP SECRET Control Officer
USERID	user identification
USTRANSCOM	United States Transportation Command
WAM PMO	WAM Program Management Office
WAM	WWMCCS ADP Modernization
WASO	WWMCCS ADP Security Officer
WASSM	WWMCCS ADP System Security Manager
WASSO	WWMCCS ADP System Security Officer
WATASO	WWMCCS ADP Terminal Area Security Officer
WIN	WWMCCS Intercomputer Network
WIND	WWMCCS Intercomputer Network Director
WNINTEL	Warning Notice--Intelligence Sources or Methods Involved
WORM	write once read many
WSC	WIN Site Coordinator
WWMCCS	Worldwide Military Command And Control System

Part II - TERMS AND DEFINITIONS

access. A specific type of interaction between a subject (i.e., a person, process or input device) and an object (i.e., an AIS resource such as a record, file, program, or output device) that results in the flow of information from one to the other. Also, the ability and opportunity to obtain knowledge of classified or sensitive but unclassified information. (DODD 5200.28)

accessible spaces.* An area within which the user controls access (with or without required clearance) and maintains an awareness of all persons entering the area. It also delineates the closest point of potential vehicular intercept.

accountability. The property that enables activities on an AIS to be traced to individuals who may then be held responsible for their actions. (DODD 5200.28)

accreditation. A formal declaration by the DAA having accreditation responsibility that the AIS is approved to operate in one or more particular security modes using a prescribed set of safeguards. Accreditation is the official management authorization for operation of an AIS and is based on the certification process and on other management considerations. The accreditation statement affixes security responsibility with the DAA and shows that due care has been taken for security. (DODD 5200.28)

AIS security. Measures and controls required to protect against unauthorized (accidental or intentional) disclosure, modification, or destruction of AISs and data and denial of service to process data. AIS security includes consideration of all hardware/software functions, characteristics, or features; operational procedures, accountability procedures, and access controls at the central computer facility, remote computer, and terminal facilities; management constraints; physical structures and devices; and personnel and communications controls needed to provide an acceptable level of risk for the AIS and for the data and information contained in the system. The totality of security safeguards needed to provide an acceptable protection level for an AIS and for data handled by an AIS. (DODD 5200.28)

assurance. A measure of confidence that the security features and architecture of an AIS accurately implement, mediate and enforce the security policy. If the security features of an AIS are relied upon to handle sensitive information and restrict user access, the features must be tested to ensure that the security policy is enforced during AIS operation. (DODD 5200.28)

audit. To conduct an independent review and examination of system records and activities to test for adequacy of system controls to ensure compliance with established policy and operational procedures and recommend changes in controls, policy, or procedures. (DODD 5200.28)

audit trail. A set of records that collectively provide documentary evidence of processing used to trace from original transactions forward to related records and reports, and/ or backwards from records and reports to their component source transactions. (DOD 5200.28-STD)

authenticate. To establish the validity of a claimed identity. (DOD 5200.28-STD)(Joint Pub 1-02)

automated information system (AIS). An assembly of computer hardware, software, or firmware configured to collect, create, communicate, compute, disseminate, process, store, or control data or information. (DODD 5200.28)

browsing. The act of searching through storage to locate or acquire information without necessarily knowing the existence or format of the information being sought. (NCSC-TG-004, Version 1)

bugging.* Implanting a physical listening or transmitting device on or in AIS hardware to gain unauthorized access to data being processed.

category. A grouping of classified or sensitive unclassified information to which an additional restrictive label is applied for signifying that personnel are granted access to the information only if they have formal access approval or other applicable authorization (e.g., proprietary information, for official use only (FOUO), compartmented information). (DODD 5200.28)

certification. The technical evaluation of an AIS's security features and other safeguards, made in support of the accreditation process, which establishes the extent that a particular AIS design and implementation meet a set of specified security requirements. (DODD 5200.28)

classification authority. The authority vested in an official of the Department of Defense to make an initial determination that information requires protection against unauthorized disclosure in the interest of national security. (DODD 5200.1-R)

classification guide. A document issued by an authorized original classifier that prescribes the level of classification and appropriate declassification instructions

for specified information to be classified derivatively. (DODD 5200.1-R)

closed security environment. An environment in which both of the following conditions hold true:

a. Application developers (including maintainers) have sufficient clearances and authorizations to provide acceptable presumption that they have not introduced malicious logic. Sufficient clearance is defined as follows: where the maximum classification of data to be processed is CONFIDENTIAL or less, developer are cleared and authorized to the same level as the most sensitive data; where the maximum classification of the data to be processed is SECRET or above, developers have at least a SECRET clearance.

b. Configuration control provides sufficient assurance that applications and the equipment are protected against the introduction of malicious logic prior to and during the operation of system applications. (NCSC-TG-004, Version 1)

communications devices.* Active or passive device dedicated to carry information among other devices and performs only that processing necessary to carry the information (e.g., networks, direct line connections).

communications security. The protection resulting from all measures designed to deny unauthorized persons information of value which might be derived from the possession and study of telecommunications, or to mislead unauthorized persons in their interpretation of the results of such possession and study. Also called COMSEC. Communications security includes a. cryptosecurity; b. transmission security; c. emission security; and d. physical security of communications security materials and information. (Joint Pub 1-02)

1. cryptosecurity - The component of communications security which results from the provision of technically sound crypto-systems and their proper use. (Joint Pub 1-02)

2. transmission security - The component of communications security which results from all measures designed to protect transmissions from interception and exploitation by means other than cryptoanalysis. (Joint Pub 1-02)

3. emission security - The component of communications security which results from all measures taken to deny unauthorized persons information of value that might be

derived from intercept and analysis of compromising emanations from crypto-equipment and telecommunications systems. (Joint Pub 1-02)

4. physical security - The component of communications security which results from all physical measures necessary to safeguard classified equipment, material, and documents from access thereto or observation thereof by unauthorized persons. (Joint Pub 1-02)

compartment. A class of information that has need-to-know access controls beyond those normally provided for access to CONFIDENTIAL, SECRET, or TOP SECRET information. (See also "Sensitive Compartment Information" and "Special Access Program.") (NCSC-TG-004, Version 1)

compromise. The known or suspected exposure of clandestine personnel, installations, or other assets or of classified information or material, to an unauthorized person. (Joint Pub 1-02)

compromising emanations. Unintentional data-related or intelligence-bearing signals that, if intercepted and analyzed, disclose the information transmission received, handled, or otherwise processed by an information processing equipment. See TEMPEST. (NCSC-TG-004, Version 1)

computer security (COMPUSEC). Synonymous with automated information security. (NCSC-TG-004, Version 1)

computer virus.* A self-propagating trojan horse, composed of three parts: a mission component, a trigger component, and a self-propagating component.

configuration control. The process of controlling modifications to the system’s hardware, firmware, software, and documentation that provides sufficient assurance that the system is protected against the introduction of improper modifications prior to, during, and after system implementation. Compare configuration management. (NCSC-TG-004, Version 1)

configuration management. The management of security features and assurances through control of changes made to a system’s hardware, software, firmware, documentation, test, test fixtures and test documentation throughout the development and operational life of the system. Compare configuration control. (NCSC-TG-004, Version 1)

controlled area.* An area within which uncontrolled movement does not permit access to classified information and which is designed for the principal purpose of providing

administrative control, safety, or a buffer area of security for limited access areas.

controlled space.* The three dimensional space surrounding equipment that processes national security information within which unauthorized personnel are:

a. Denied unrestricted access.

b. Enter escorted by authorized personnel or under continual physical or electronic surveillance.

controlled zone.* The space, expressed in feet of radius, surrounding equipment processing sensitive information, that is under sufficient physical and technical control to preclude an unauthorized entry or compromise.

control zone. The space, expressed in feet of radius, surrounding equipment processing sensitive information, that is under sufficient physical and technical control to preclude an unauthorized entry or compromise. (NCSC-TG-004, Version 1)

COTS software.* Software acquired by government contract through a commercial vendor. This software is a standard product, not developed by a vendor for a particular government project.

countermeasure. Any action, device, procedure, technique, or other measure that reduces the vulnerability of or threat to a system. (NCSC-TG-004, Version 1)

CSMA-CD.* A line protocol commonly used on very high speed LANs.

customer (WIN Customer).* Person or organization that receives products from the WIN but does not have access (see Access). (Does not include those persons or organizations defined as WIN users.) A WIN customer does not require a USERID or Password.

DAO Code.* Department/Agency/Organization code. A programmable code used by the STU-III to identify incoming callers against a predefined access list.

data. A representation of facts, concepts, information, or instructions suitable for communication, interpretation, or processing by humans or by an AIS. (DODD 5200.28)

data integrity. The state that exists when data is unchanged from its source and accidentally or maliciously has not been modified, altered, or destroyed. (DODD 5200.28)

data owner. The authority, individual, or organization who has original responsibility for the data by statute, Executive Order, or Directive. (DODD 5200.28)

declassification. The determination in the interests of national security, classified information no longer requires any degree of protection against unauthorized disclosure, coupled with removal or cancellation of the classification designation. (Joint Pub 1-02)

declassification (of ADP Magnetic Storage Media).* A procedure which will totally remove all the classified or sensitive information stored on magnetic media followed by a review of the procedure performed. A decision can then be made for (or against) actual removal of the classification level of the media. Declassification allows release of the media from the controlled environment if approved by the appropriate authorities.

dedicated security mode. A mode of operation wherein all users have the clearance or authorization and need-to-know for all data handled by the AIS. If the AIS processes special access information, all users require formal access approval. In the dedicated mode, an AIS may handle a single classification level and/or category of information or a range of classification levels and/or categories. (DODD 5200.28)

Defense Data Network (DDN).* A DISA program (replacing the canceled DSN II program) to establish a state-of-the-art, generalized data communications network for DOD activities. The DDN is intended to subsume all existing DOD data networks, including the WINCS, MILNET, IDHS-C, and DSN. The WINCS will be merged into the DDN as the TOP SECRET portion of the network, and the WIN will continue to exist as a DDN user. (DISA Circular 370-P185-15) Currently, the DDN has four independent subnetworks: MILNET is an unclassified E-mail; DSNET1 is a SECRET high network; DSNET2 is a TOP SECRET system high network designated for the WIN; and DSNET3 is a TS/SCI network. In the future, the DDN will employ the BLACKER-on-host approach to mediate different classes of information.

DSNET2.* The worldwide communications network that provides secure (TOP SECRET) interconnection of WIN multiuser hosts.

degauss.* Destroy information contained in magnetic media by subjecting that media to high intensity alternating magnetic fields, following which, the magnetic fields slowly decrease.

degausser products list (DPL). A list of commercially produced degaussers that meet National Security Agency specifications. This list is included in the NSA Information Systems Security Products and Services Catalogue, and is available through the Government Printing Office. See INFOSEC catalog. (NCSC-TG-004, Version 1)

denial of service. Action or actions that result in the inability of an AIS or any essential part to perform its designated mission, either by loss or degradation of operational capability. (DODD 5200.28)

Department/Agency/Organization Codes.* Programmable codes used by a receiving STU-III enabling it to discriminate between groups of callers and allowing access only to those whose DAO code is programmed into the receiver's STU-III.

designated approving authority (DAA). The official who has the authority to decide on accepting the security safeguards prescribed for an AIS or the official who may be responsible for issuing an accreditation statement that records the decision to accept those safeguards. The DAA must be at an organizational level, have authority to evaluate the overall mission requirements of the AIS, and to provide definitive directions to AIS developers or owners relative to the risk in the security posture of the AIS. (DODD 5200.28)

designated development activity (DDA).* The activity assigned responsibility by the Joint Staff, J-6, for development of a WWMCCS standard software capability.

discretionary access control (DAC). A means of restricting access to objects based on the identity and need-to-know of the user, process and/or groups to which they belong. The controls are discretionary in the sense that a subject with a certain access permission is capable of passing that permission (perhaps indirectly) on to any other subject. Compare mandatory access control. (NCSC-TG-004, Version 1)

downgrade. To determine that classified information requires, in the interests of national security, a lower degree of protection against unauthorized disclosure than currently provided, coupled with a changing of the classification designation to reflect such lower degree. (Joint Pub 1-02)

Downgrading (of Magnetic Storage Media).* A procedure used under the system high (e.g., TOP SECRET) mode of operation, which will reclassify the magnetic storage media to reflect the true (actual) classification of classified or sensitive information stored.

emanations security.* The protection that results from all measures designed to deny unauthorized persons information of value that might be derived from intercept and analysis of compromising emanations.

evaluated products list (EPL). A documented inventory of equipments, hardware, software, and/or firmware that have been evaluated against the evaluation criteria found in DOD 5200.28-STD. (DODD 5200.28)

firmware.* Software that is permanently stored in a hardware device that allows reading of the software but not writing or modifying. The most common device for firmware is ROM.

gateway.* A device or system that enables the passage of data between networks. In the WIN, DSN terminals such as AMME, AF/AMPE, and LDMX, which allow WIN multiuser hosts to connect to the DSN network, may be considered gateways.

group USERID.* A USERID shared by more than one authorized users. Also implies sharing of the associated TOP SECRET password.

guard. A processor that provides a filter between two systems operating at different security levels or between a user terminal and a database to filter out data that the user is not authorized to access. (NCSC-TG-004, Version 1)

inadvertent disclosure.* Accidental exposure of classified defense information to a person not authorized access. This may result in a compromise or a need-to-know violation.

incident. See security incident.

individual accountability. The ability to associate positively the identity of a user with the time, method, and degree of access to a system. (NCSC-TG-004, Version 1)

information systems security.* A composite of the means of protecting telecommunications systems and automated information systems and the information they process.

integrity, AIS.* The capability of an AIS to perform its intended function in an unimpaired manner, free from deliberate or inadvertent unauthorized manipulation of the system. Inherent quality of protection that ensures and maintains the security of entities of an AIS.

intelligent terminal. A terminal that is programmable, able to accept peripheral devices, able to connect with other terminals or computers, able to accept additional memory, or

which may be modified to have these characteristics. (DODD 5200.28)

least privilege. The principle that requires that each subject be granted the most restrictive set of privileges needed for the performance of authorized tasks. The application of this principal limits the damage that can result from accident, error, or unauthorized use. (NCSC-TG-004, Version 1)

local area network.* A short-haul data communications system that connects ADP devices in a building or group of buildings within a few square kilometers, including (but not limited to) workstations, front-end processors, controllers, switches, and gateways.

mandatory access control (MAC). A means of restricting access to objects based on the sensitivity (as represented by a label) of the information contained in the objects and the formal authorization (i.e., clearance) of subjects to access information of such sensitivity. Compare discretionary access control. (NCSC-TG-004, Version 1)

multilevel security (MLS) mode. A mode of operation that allows two or more classification levels of information to be processed simultaneously within the same system when not all users have a clearance or formal access approval for all data handled by the AIS. (DODD 5200.28)

multilevel security.* Concept of processing information with different classifications and categories that simultaneously permits access by users with different security clearances but prevents users from obtaining access to information for which they lack authorization.

multiuser hosts.* A computer with a multiprocessing operating system that performs processing for more than one user simultaneously. The DPS-8000 is an example of a multiuser host. A WIN site can consist of one multiuser host or several, depending on the site mission, organization, and facility(s).

need to know. A determination made in the interest of U.S. national security by the custodian of classified or sensitive unclassified information, which a prospective recipient has a requirement for access to, knowledge of, or possession of the information to perform official tasks or services. (DODD 5200.28)

need-to-know violation.* The disclosure of classified and sensitive unclassified defense information to a person who is cleared for the information but has no requirement for such information to carry out assigned official duties.

network. A network is composed of a communications medium and all components attached to that medium whose responsibility is the transference of information. Such components may include AISs, packet switches, telecommunications controllers, key distribution centers, and technical control devices. (DODD 5200.28)

network operations center (NOC).* An operating center that operates 24 hours a day within the Pentagon and constantly monitors network status and coordinates network operations. This network coordination center supports the activities of the NMCC, WIND, WASO, and WIN users.

nonprocessing input and output devices.* A device used to enter information and commands into a multiuser host computer and receive information from the host, but performs no processing itself (e.g., simple, memoryless terminals).

nonvolatile memory.* Memory (such as semiconductor memory) that does not lose its memory retention capability when electric power is removed.

object. A passive entity that contains or receives information. Access to an object potentially implies access to the information it contains. Examples of objects are: records, blocks, pages, segments, files, directories, directory trees, and programs, as well as bits, bytes, words, fields, processors, video displays, keyboards, clocks, printers, network nodes. (NCSC-TG-004, Version 1)

object reuse. The reassignment and reuse of a storage medium (e.g., page frame, disk sector, magnetic tape) that once contained one or more objects. To be securely reused and assigned to a new subject, storage media must contain no residual data (magnetic remanence) from the object(s) previously contained in the media. (NCSC-TG-004, Version 1)

open security environment. An environment that includes those systems in which at least one of the following conditions holds true: (a) Application developers (including maintainers) do not have sufficient clearance or authorization to provide an acceptable presumption that they have not introduced malicious logic. (b) Configuration control does not provide sufficient assurance that applications are protected against introduction of malicious logic prior to and during the operation of system applications.(NCSC-TG-004, Version 1)

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 when it is not occupied by authorized personnel.

operating system.* An integrated collection of service routines for supervising the sequencing and processing of programs by a computer. Operating systems control the allocation of resources to users and their programs and play a central role in assuring the secure operation of a computer system. Operating systems may perform input or output accounting, resource allocation, storage assignment tasks, and other system related functions (synonymous with monitor, executive, control program, and supervisor).

operational performance data (Network).* A measure of the effectiveness of the WIN as seen by a user in relationship to the accomplishment of his job. Typically expressed in terms of success rate (with regard to job completion; e.g., transferring a file or accessing an application in a remote multiuser host), speed of service (system responsiveness or time required to complete a job), and accuracy.

output-only devices.* Devices, such as printers, connected to a multiuser host (directly or through communications devices) that perform no input functions to the host.

overwrite.* A procedure to remove or destroy data recorded on magnetic storage media by writing patterns of data over or on top of the data stored on the media.

packet switched network.* A communications network that breaks down all message or data traffic into standardized "packets" and individually routes these packets to their destination. This routing is performed by a combination of an address contained in these message header and a dynamic routing algorithm maintained by the network. The DDN, WINCS, ARPANET, and MILNET are all packet-switched networks.

packet switching node (PSN).* A communications processor or packet switch used to link each multiuser host to the dedicated WIN communications sub-network. The complete network is formed by interconnecting the PSNs through wideband commercial lines secured by cryptographic equipment. Each PSN is programmed as a packet switch to forward messages to other PSNs in the network until the message reached the destination multiuser host.

partitioned security mode. A mode of operation wherein all personnel have the clearance, but not necessarily formal access approval and need-to-know, for all information handled by the AIS. This security mode encompasses the compartmented mode defined in DCID Number 1/16. (DODD 5200.28)

password. A protected/private character string used to authenticate an identity. (NCSC-TG-004, Version 1)

penetration. The successful act of bypassing the security mechanisms of a system. (NCSC-TG-004, Version 1)

penetration testing. The portion of security testing in which the evaluators attempt to circumvent the security features of a system. The evaluators may be assumed to use all system design and implementation documentation, which may include listings of system source code, manuals, and circuit diagrams. The evaluators work under the same constraints applied to ordinary users. (NCSC-TG-004, Version 1)

periods processing. A manner of operating an AIS in which the security mode of operation and/or maximum classification of data handled by the AIS is established for an interval of time or period) and then changed for the following interval of time. A period extends from any secure initialization of the AIS to the completion of any purging of sensitive data handled by the AIS during the period. (DODD 5200.28)

privileged function.* A function that requires that a user or program have unrestricted access to the operating system, applications programs, or data, whether in memory or on media.

privileged state.* A state in which a user or program has unrestricted access to the operating system, applications programs, or data, whether in memory or on media.

privity.* A privileged mode of operation wherein all instructions are operative, giving complete and unrestricted control of the system.

protected distribution system.* A telecommunications system to which acoustical, electrical, electromagnetic, and physical safeguards have been applied to permit its use for secure electrical or optical transmission of unencrypted classified information or sensitive unclassified information.

public domain software.* Software acquired from government or nongovernment sources, often at no charge, when the source takes no responsibility for the integrity or maintenance of the software.

purge. Removal of sensitive data from an AIS at the end of a period of processing, including from AIS storage devices and other peripheral devices with storage capacity, in such a way that there is assurance proportional to the sensitivity of the data that the data may not be reconstructed. An AIS must be disconnected from any external network before a purge. (DODD 5200.28)

read access. Permission to read information. (NCSC-TG-004, Version 1)

read-only memory (ROM).* A storage area in which the contents can be read but not altered during normal computer processing.

RED/BLACK concept.* The concept that electrical and electronic circuits, components, equipment, systems, and so forth that handle classified plain language information in electrical signal form (RED) be separated from those that 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. To determine that certain classified information requires, in the interest of national defense, a higher or a lower degree of protection against unauthorized disclosure than currently provided, coupled with a changing of the classification designation to reflect such higher or lower degree. (Joint Pub 1-02)

remote DATANET-8/Concentrator/LAN sites.* Sites used as terminal concentrators with the additional ability to directly connect to a PSN as well as a multiuser host computer. This affords the user opportunity to travel the WINCs and access up to four different multiuser hosts without using the current TELNET features. These remote sites require security and WIN site management similar to RNP sites.

remote network processor (RNP). See WIN RNP.

remote terminal area.* Remote computer facilities, peripheral devices, or terminals located outside the central computer facility.

residue. Data left in storage after processing operations are complete, but before degaussing or rewriting has taken place. (NCSC-TG-004, Version 1)

risk. A combination of the likelihood that a threat shall occur, the likelihood that a threat occurrence shall result in an adverse impact, and the severity of the resulting adverse impact. (DODD 5200.28)

risk analysis. An analysis of system assets and vulnerabilities to establish an expected loss from certain events based on estimated probabilities of occurrence. (DODD 5200.28)

risk analysis. The process of identifying security risks, determining their magnitude, and identifying areas needing safeguards. Risk analysis is a part of risk management. Synonymous with risk assessment. (NCSC-TG-004, Version 1)

risk management. The total process of identifying, controlling, and eliminating or minimizing uncertain events that may affect system resources. It includes risk analysis, cost-benefit analysis, selection, implementation and test, security evaluation of safeguards, and overall security review. (NCSC-TG-004, Version 1)

safeguard statement.* A statement affixed to a computer output that states the highest classification being processed at the time product was produced and which requires its control at that level until a responsible person can determine its true classification.

sanitize.* To erase or overwrite classified data stored on magnetic media for the purpose of declassifying the media.

security incident.* An incident involving classified information in which there is a deviation from the requirements of governing security regulations (e.g., compromise, inadvertent disclosure, need-to-know violation, and administrative deviation).

security mode. A mode of operation in which the DAA accredits an AIS to operate. Inherent with each of the four security modes (dedicated, system high, multilevel, partitioned) are restrictions on the user clearance levels, formal access requirements, need-to-know requirements, and the range of sensitive information permitted on the AIS. (DODD 5200.28)

security-relevant event.* Any event that attempts to violate the security policy of the system (e.g., too many attempts to logon).

security technical procedure (STP).* A document published to furnish procedural guidance in a specific area to aid in implementing the policy of Joint Pub 6-03.7.

security test and evaluation (ST&E). An examination and analysis of the security safeguards of a system as they have been applied in an operational environment to determine the security posture of the system.(NCSC-TG-004, Version 1)

sensitive compartmented information (SCI). Classified information about or derived from intelligence sources, methods, or analytical processes that is required to be handled exclusively within formal access control systems

established by the Director, Central Intelligence. (DODD 5200.28)

sensitivity label. A piece of information that represents the security level of an object. Sensitivity labels are used by the TCB as the basis for mandatory access control decisions. (NCSC-TG-004, Version 1)

single-user hosts.* Host computers (e.g., workstations) that perform processing for only one user at a time (this does not preclude multiple users over time).

SIOP-ESI. An acronym for Single Integrated Operational Plan-Extremely Sensitive Information, A DOD Special Access Program. (DODD 5200.28)

site (WIN site or WIN multiuser host site).* A single geographic location of one or more multiuser hosts that are connected to the WIN. A DOD command, agency, or activity employing ADPE and communications equipment described as a WIN multiuser host, WIN RNP, or Remote DATANET-8/Concentrator/LAN to establish WIN connectivity. A WIN site may consist of one or more WIN Elements. If a LAN gateway is employed for inter-WIN site connection, an SDN must be submitted.

special access programs. Any program imposing need-to-know or access controls beyond those normally required for access to CONFIDENTIAL, SECRET, or TOP SECRET information. Such a program includes, but is not limited to, special clearance or investigative requirements, special designation of officials authorized to determine need to know, or special lists of persons determined to have a need to know. (DODD 5200.28)

stand-alone (shared system). A system that is physically and electrically isolated from all other systems and is intended to be used by more than one person, either simultaneously (e.g., a system with multiple terminals) or serially, with data belonging to one user remaining available to the system while another user is using the system (e.g., a personal computer with nonremovable storage media such as a hard disk.) (NCSC-TG-004, Version 1)

star network.* A communications network with a central hub that normally performs message routing between host computers and terminals. Each WIN multiuser host is the hub of a Star network, with connections to as many as 400 terminals.

subject. An active entity, generally in the form of a person, process, or device that causes information to flow

among objects or changes the system state. Technically, a process/domain pair. (NCSC-TG-004, Version 1)

system access.* Refers to access privileges given to maintainers of the operating system files or, more frequently, the generic term for users' capability to logon to a computer system or network.

system high security mode. A mode of operation wherein all users having access to the AIS possess a security clearance or authorization, but not necessarily a need to know, for all data handled by the AIS. If the AIS processes special access information, all users must have formal access approval. (DODD 5200.28)

system users.* Those individuals with direct connections to the system and also those individuals without direct connections who receive output or generate input that is not reliably reviewed for classification by a responsible individual. The clearance of system users is used in the calculation of risk index.

tamper-indicative seal.* A special seal, approved by NSA, that can be used to seal physical objects, such as ADP terminal workstations. The unauthorized removal of such a seal is clearly recognizable.

technical performance data.* A measure of the effectiveness of WIN components (hardware, software, communications, etc.), both individually and collectively. Typically expressed in terms of availability or reliability, mean-time between incident, and mean-time to service.

technical vulnerability. A hardware, firmware, communication, or software flaw that leaves a computer processing system open for potential exploitation, either externally or internally, thereby resulting in risk for the owner, user, or manager of the system. (NCSC-TG-004, Version 1)

TEMPEST. The study and control of spurious electronic signals emitted by electrical equipment. (NCSC-TG-004, Version 1)

terminal access controller (TAC).* A component of a packet switched network similar to a PSN, but which provides direct terminal access to the network instead of multiuser host access. It also provides intermediate switching points for in-transit data. ARPANET and MILNET provide this capability, but WIN does not (for improved security).

threat. Any circumstance or event with the potential to cause harm to a system in the form of destruction,

disclosure, modification of data, and/or denial of service. (NCSC-TG-004, Version 1)

time bomb.* A variant of the trojan horse, whereby malicious code is inserted to be automatically triggered at some future time.

token passing.* A line protocol sometimes used on Local Area Network as an alternative to CSMA-CD.

trap door. A hidden computer software or hardware mechanism that can be triggered to permit system protection mechanisms to be circumvented. It is activated in some innocent-appearing manner; e.g., a special "random" key sequence at a terminal. Software developers often introduce trap doors in their code that enable them to reenter the system and perform certain functions. Synonymous with back door. (NCSC-TG-004, Version 1)

Trojan Horse.* A computer program with an apparently or actually useful function that contains additional (hidden) functions that surreptitiously exploit the legitimate authorizations of the invoking process to the detriment of security. For example, making a "blind copy" of a sensitive file for the creator of the trojan horse. A Trojan horse is a piece of computer code which has an ostensible legitimate and useful function, such as a sort or merge routine or regression analysis package. It also contains a hidden function, such as copying files or changing access control parameters. The trojan horse is then presented to an authorized user as a useful and desirable function which, when it is executed, also carries out its covert function, potentially undetected.

Trusted Computer System (TCS). A system that employs sufficient hardware and software assurance measures to allow its use for simultaneous processing of a range of sensitive or classified information. (NCSC-TG-004, Version 1)

Trusted Computing Base (TCB). The totality of protection mechanisms within a computer system, including hardware, firmware, and software, the combination of which is responsible for enforcing a security policy. A TCB consists of one or more components that together enforce a unified security policy over a product or system. The ability of a TCB to enforce correctly a unified security policy depends solely on the mechanisms within the TCB and on the correct input by system administrative personnel of parameters (e.g., a user’s clearance level) related to the security policy. (NCSC-TG-004, Version 1)

Trusted Computer System Evaluation Criteria (TCSEC).* A document published by the National Computer Security Center

containing a uniform set of basic requirements and evaluation classes for assessing degrees of assurance in the effectiveness of hardware and software security controls built into systems. These criteria are intended for use in the design and evaluation of systems that will process or store sensitive or classified data. This document is DOD 5200.28-STD and is alternately referred to as the Criteria or The Orange Book.

trusted path. A mechanism by which a person at a terminal can communicate directly with the Trusted Computing Base. This mechanism can only be activated by the person or the Trusted Computing Base and cannot be imitated by untrusted software. (NCSC-TG-004, Version 1)

trusted software.* The software portion of a Trusted Computing Base. Software, usually affecting system security, that has been certified to perform as specified. Certification may be performed by an organization the accreditor deems appropriate, depending on the situation.

TSCM inspection.* A limited technical security countermeasures area or technical examination of specific item, such as a newly installed telephone, to detect hostile attempts at technical penetration.

type accreditation.* Official authentication by the DAA to employ a system in a specified environment. This authorization includes a statement of residual risk, delineates operating environment, and specific use. It is performed when multiple copies of a system are to be fielded.

User (or WIN User).* A person who interacts directly with a computer system. In the WIN, a person or organization who has access to a WIN through a remote device or who is allowed to submit input to the system thorough other media; e.g., tape or floppy disk, and has been assigned an individual or group USERID and password. (Does not include those persons or organizations defined as customers.)

virus. See computer virus.

volatile memory.* Memory (such as semiconductor memory) that loses its retention capability when electronic power is removed.

vulnerability.* A weakness in system security procedures, system design, implementation, internal controls, etc., that could be exploited to violate system security policy. (NCSC-TG-004, Version 1) The susceptibility of a particular system to a specific attack, along with the opportunity available to a hostile entity 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.

WIN.* A centrally managed information processing and exchange communications system designed to serve the needs of the NCA, Joint Chiefs of Staff, CINCs, Services, and Directors of selected Defense agencies. The WIN employs a suite of WIN multiuser hosts with standard operating systems and applications software, network monitoring facilities, RNPs, LANs, terminals, intelligent workstations, and peripheral devices interconnected through the facilities of the DSNET2. The WIN concept includes an aggregation of WWMCCS computers, WIN standard applications, command unique applications, communications, reporting systems, and procedures.

WIN Communications Subsystem (WINCS).* The physical interlinking portion of the WIN, consisting of BBN C/30 PSN's and their associated interconnecting communications circuits. It does not include the hardware or software for the communications front-end processors that interface the WIN multiuser host computers to the WINCS. The WINCS is a high speed packet switched network based on ARPANET technology. It differs from most other packet switched networks in that it provides no direct terminal access. All user terminals are connected to WIN multiuser hosts and must pass a multiuser host security check before network access is permitted. The WINCS is currently administered by a DISA DDN program and will eventually become part of the unified DDN system. Security policy in this document does not apply directly to the WINCs, but as agreed upon in the MOA between the WIN DAA and DISA.

write access. Permission to write an object. (NCSC-TG-004, Version 1)

WWMCCS ADP Security Officer (WASO).* The Joint Staff officer responsible to the WIN DAA to ensure that proper security measures are implemented and adhered to by all elements of the WIN. The WASO is appointed by the Director, J-6, Joint Staff.

WWMCCS ADP System Security Manager (WASSM).* Person with command responsibility for making WIN multiuser host site computer system security policy and with adequate authority to ensure that INFOSEC activities, policies, and directives are enforced and conflicts of interest, responsibilities, and functions are resolved. (NOTE: A WASSM need not be physically located at a WIN multiuser host site for which he or she is responsible.)

WWMCCS ADP System Security Officer (WASSO).* The WIN site official responsible to the WIN site DAA for ensuring that proper security measures are implemented and adhered to by all elements of the WIN site. The WASSO is the focal point for WIN site security matters and is appointed by the WIN site DAA. The WASSO also is responsible for all WASSM duties when a WASSM is not appointed.

WIN customer. See customer.

WIN element.* The WIN and communications entities, both hardware and software that, when operated together, form an operational entity. The WIN elements include WIN multiuser host computers, workstations, terminals, printers, PSNs, LANs, or other WIN communications connection devices and the systems and applications software that are operated on these WIN devices.

WIN multiuser host.* A WIN site that achieves network connectivity through a direct interface with the DSNET2 system. Multiple multiuser hosts may be located at a WIN site.

WIN Remote Network Processor (RNP).* A WIN site that achieves network connectivity through the communications interfaces available to a WIN multiuser host. A WIN RNP may be as sophisticated as a minicomputer or as simple as a concentrator, a collection of WIN terminals. Classification of a WIN site as a multiuser host or RNP is based solely on the manner in which network connectivity is established. If connectivity is established directly through the DSNET2, the site is a multiuser host. If DSNET2 connectivity is established indirectly through a multiuser host, the site is an RNP. No statement of command relationship is implied as a result of a WIN site being a multiuser host or an RNP. In some cases, an RNP may be the senior command echelon. In these cases, operations of the WIN multiuser host must not adversely affect the prerogatives of the senior commander, and the senior commander must not jeopardize the network operations and security responsibilities incumbent on the multiuser host site commander. Addition of an RNP to a WIN multiuser host connection is the authority of the WIN multiuser host DAA (local DAA). However, it must be identified in the ST&E report.

WIN Site.* A DOD command, agency, or activity employing ADPE and communications equipment described above to establish WIN connectivity. If non-WIN standard components are employed, an SDN must be submitted.

WIN user. See user.

WNINTEL. This marking may be used only on intelligence that identifies or would reasonably permit identification of an intelligence source or method that is susceptible to countermeasures that could nullify or reduce its effectiveness. In order to avoid confusion as to the extent of dissemination and use restrictions governing the information involved, the WNINTEL label must not be used in conjunction with SAPIs or SCI controls since they are included under the definition of this marking. (DCID 1/16)

_____

* This term or definition is applicable only in the context of this pub and cannot be referenced outside of this publication.