DOCID: 3978833
Approved for Release by NSA on 06-14-2012 pursuant to E.O. 13526

# NATIONAL SECURITY AGENCY
# CENTRAL SECURITY SERVICE
FORT GEORGE G. MEADE, MARYLAND

NSA/CSS DIR. NO. 10-27*
DATE: 30 November 1979

# NSA/CSS DIRECTIVE

## SECURITY REQUIREMENTS FOR AUTOMATIC DATA PROCESSING (ADP) SYSTEMS


| | SECTION |
|---|---|
| REFERENCES | I |
| DEFINITIONS | II |
| PURPOSE AND APPLICABILITY | III |
| POLICY | IV |
| RESPONSIBILITIES | V |
| IMPLEMENTATION | VI |


## SECTION I - REFERENCES

1. References:

a. DoD Directive No. 5200.28, "Security Requirements for Automatic Data Processing (ADP) Systems," dated 29 April 1978.

b. DCID No. 1/16, "Security of Foreign Intelligence in Automated Data Processing Systems and Networks," (C) dated 6 June 1978.

c. OMB Circular A-71, Transmittal Memorandum No. 1, "Security of Federal Automated Information Systems," dated 27 July 1978.

d. NSA Manual 90-4, "ADP Security Design and Operating Standards," (to be published).

e. NSA/CSS Circular 90-10, "TEMPEST Control Considerations for SIGINT Installations," dated 3 March 1976.

## SECTION II - DEFINITIONS

2. The following definitions apply to terms used in this directive:

*This Directive supersedes NSA/CSS Directive Number 10-27(U), dated 25 October 1974

OPI: [redacted]

P.L. 86-36

DOCID: 3978833



a. ADP System Approval - The formal approval by the Designated Approving Authority (DAA) of ADP systems and networks for the processing, use, storage, and production of material under the jurisdiction of NSA/CSS. The approval is based upon the testing, evaluation, and formal accreditation of the system to verify the application of appropriate security measures to satisfy the requirements contained in the references.

b. Accreditation - The formal declaration that an ADP system or network provides an acceptable level of protection for processing sensitive data in an operational environment. Accreditation is based upon formal certifications from the Chiefs of Key Components and Field Elements, in accordance with responsibilities assigned under this Directive, that they have conducted evaluations employing criteria contained in the references, and the extent to which the system or network meets these criteria.

c. Certification - The technical evaluation that establishes the extent to which a particular computer system or network design and implementation meet the requirements prescribed in the references.

d. Communications Security - Protective measures taken to deny unauthorized persons information derived from telecommunications of the United States Government related to national security and to ensure the authenticity of such communications. Such protection results from the application of security measures (including cryptosecurity, transmission security, emissions security) to electrical systems generating, handling, processing, or using national security or national security related information. It also includes the application of physical security measures to communications security information or materials.

e. Additional terms relative to ADP security are contained in Enclosure 2 to reference a. and the Glossary to reference b.

## SECTION III - PURPOSE AND APPLICABILITY

3. This directive implements the provisions of references a. and b. as they apply to NSA/CSS, establishes policy, assigns responsibilities to ensure that NSA/CSS ADP systems and those of its contractors meet security requirements, and documents the NSA/CSS responsibility for providing Communications Security (COMSEC) assistance to other U.S. Government components in support of effective ADP security measures. Its provisions are applicable to all NSA/CSS Components, worldwide.

## SECTION IV POLICY

4. All ADP systems under the cognizance of the Director, NSA/Chief, CSS will conform with the security specifications contained in the references. The security levels identified in reference d. apply to all equipments (including telecommunications computers) used to store, process, or communicate classified cryptologic or related information, including those equipments in use by NSA/CSS contractors.

DOCID: 3978833



5. All personnel data, management data, and national security-related information in NSA/CSS ADP systems, while not necessarily classified, shall be protected by use of adequate and practical software/hardware safeguards and management procedures.

6. The security policy contained in references a. and b. shall be judiciously implemented to assure effective use of NSA/CSS ADP systems and those of its contractors who process classified and other specified material.

7. NSA/CSS systems will be connected to ADP systems of another Government component, a non-government ADP system, or a contractor facility only after prior NSA/CSS review to ensure that the inter-connected systems meet NSA/CSS security requirements.

8. Remote terminals and peripheral devices connected to an NSA/CSS ADP system will be considered part of the NSA/CSS ADP system. In order to ensure that NSA/CSS security requirements are met, a technical evaluation and formal certification must be provided, attesting that the terminals and devices, and the areas in which they are located, meet NSA/CSS security requirements. When such terminals and devices are connected to more than one NSA/CSS ADP system, the security requirements highest among the associated systems must be met.

9. In some cases, responsibilities for ADP security overlap NSA/CSS organizational lines, with several organizations having an interest in certain areas. It is incumbent upon the organization to which primary responsibility has been assigned to effect coordination with organizations having an interest in such areas.

## SECTION V - RESPONSIBILITIES

10. Under the provisions of references a. and b., the Director, NSA/Chief, CSS (or, in his absence, the Deputy Director, NSA) is the Designated Approving Authority (DAA) for any NSA/CSS ADP system. The Deputy Director, NSA, is authorized to act as the DAA for NSA/CSS ADP systems not operating in the Compartmented Mode as defined in reference b. The DAA will:

a. Approve all NSA/CSS ADP systems for the processing, use, storage and production of classified and other specified information.

b. Authorize temporary exceptions of up to one year to specific ADP security measures that would impair operation and mission effectiveness, provided that continuous progress is made toward ultimate compliance.

11. The Deputy Director for Telecommunications and Computer Services (DDT), (designated separately as the Senior ADP Policy Official (SADPPO)) will:

DOCID: 3978833



a. Accredit the operation of NSA/CSS ADP systems for the processing, use, storage, and production of classified and other specified material based upon information provided in accordance with paragraphs 12 through 18 below.

b. Assure that NSA/CSS ADP systems and those of its contractors continuously meet the security requirements prescribed and that continued approval of each system is based upon the results of a recurring review, testing, and favorable evaluation of the security features.

c. Act as the focal point to monitor and coordinate all aspects of the security of NSA/CSS ADP systems.

d. Control and administer the NSA/CSS ADP Security Officer Program to ensure that information, system, and network security officers are designated, informed of their duties and responsibilities, trained in and advised of the latest ADP security technology and procedures, and provided necessary security support and assistance.

e. Approve the adequacy of the plans for the security of each NSA/CSS ADP system being developed or procured.

f. Develop an NSA/CSS reporting system to provide the Director, NSA/Chief, CSS with basic data on the status of the security of NSA/CSS ADP systems, including problems and corrective actions needed or in process, as well as an inventory of ADP terminals available for each control zone.

g. In conjunction with other NSA/CSS components, arrange appropriate NSA/CSS representation on national and DoD committees, boards, panels or working groups concerned with ADP security. Representation on any committee, board, panel, or working group whose primary interest is the technical aspects of ADP security shall be concurred in by DDC.

h. Ensure that ADP security techniques and procedures developed by DDO, DDR, DDC and other NSA/CSS Key Components, and validated by DDC, are incorporated into existing and planned NSA/CSS ADP systems and networks.

i. Approve the connection of other U.S. Government component or contractor ADP systems to NSA/CSS ADP systems and networks, based on evaluations of the external systems by DDC and DDM.

j. Secure the approval of the ADPR on all security requirements affecting ADP systems that process fiscal and accounting data.

12. The Deputy Director for Communications Security (DDC) serves as the principal technical advisor to the Director, NSA/Chief, CSS on ADP security and will:

a. Certify, in the formal accreditation process, that ADP systems under the authority of NSA/CSS have satisfied the minimum COMSEC, as well as software and hardware security requirements prescribed in the references.

DOCID: 3978833



b. Establish minimum COMSEC, software, and hardware security requirements and identify security threats to NSA/CSS ADP systems.

c. Perform vulnerability and countermeasure analyses on selected ADP systems and provide technical guidance for correction of the insecurities detected. Selection of systems and performance of their analyses will be done in collaboration with the Chiefs of Key Components and Analysis Groups responsible for the ADP activities.

d. Periodically review and evaluate security capabilities of NSA/CSS ADP systems, in coordination with the responsible Chief of a Key Component or Analysis Group, to determine the adequacy of security access controls, including the use of passwords and security audit trails and, where necessary, develop new or improved controls.

e. In conjunction with other NSA/CSS Key Components, prescribe standards and techniques by which security features of ADP systems under the jurisdiction of NSA/CSS will be tested and evaluated and assist user organizations in prescribing standards and techniques for their systems.

f. Evaluate and approve cryptography to be used in NSA/CSS ADP systems.

g. Provide COMSEC assistance in support of effective ADP security to other U.S. Government components, upon request.

h. Publish and maintain, in coordination with NSA/CSS Key Components, reference d. as the standard for certification and accreditation of all ADP systems that handle, process, or store classified cryptologic information.

Routing for Tech dept in CSC

i. Certify to DDT that ADP systems of other U.S. Government components or contractors, which are to be connected to NSA/CSS ADP systems or networks, have satisfied the minimum COMSEC, as well as software and hardware security requirements.

13. The Deputy Director for Operations (DDO) will:

a. Ensure that SIGINT data sets and bases are secured by properly utilizing ADP system security mechanisms and protective features required in the references and this Directive.

b. Authorize access to SIGINT product data sets/bases.

c. Support the advancement of methodologies and techniques, and establish plans, procedures, and monitoring mechanisms to provide access and security safeguards for SIGINT product data sets/bases.

DOCID: 3978833



14. The Deputy Director for Research and Engineering (DDR) will:

a. In coordination with DDT and DDC, conduct a continuing program of research into ADP system and network vulnerabilities, security techniques, and effective countermeasures.

b. Perform research and develop methods and techniques for secure software development and verification.

c. Develop and influence the development of effective ADP security measures for operating systems and application subsystems in coordination with DDT and DDC.

d. Develop communications security equipment and techniques for ADP networks and remote user terminals in coordination with DDC.

e. Incorporate adequate measures and support into systems and networks being planned and developed to assure effective ADP system and network security.

15. The Deputy Director for Management Services (DDM) will:

a. Establish and promulgate physical and personnel security standards necessary to provide adequate safeguards and controls for access to NSA/CSS ADP areas.

b. Certify to DDT that ADP facilities of both NSA/CSS and its contractors meet current physical security standards.

c. Certify to DDT that ADP facilities of other U.S. Government components or contractors, which are to be connected to NSA/CSS ADP systems or networks, meet current physical security standards.

16. The Assistant Director for Policy and Liaison (ADPL) will:

a. Maintain an overview of the policy aspects of ADP systems security.

b. Collaborate in any ADP security program when policy matters involving sensitive operations are concerned.

17. The Assistant Director for Plans and Resources (ADPR) will secure General Accounting Office approval for all procedures affecting NSA/CSS ADP systems that process fiscal and accounting data and will advise DDT that approval has been received.

18. The Chiefs of the Key Components and the Chiefs of the Field Components who develop, manage, operate, or are otherwise responsible for ADP systems will:

DOCID: 3978833



a. In collaboration with DDC and DDT, assure that ADP systems to be developed, procured, leased, or utilized, provide adequate security safeguards for classified and other specified information to be contained in the system.

b. Assure that those ADP systems already designed for future placement and those systems already installed conform to the security requirements of reference d. and, if not, bring them into compliance with the standards prescribed at the earliest possible date.

X c. Assure that security measures for peripheral devices or remote terminals and the areas in which the devices or remote terminals are located meet NSA/CSS security requirements.

d. Test, evaluate and monitor the security integrity of ADP systems and collaborate with DDT, DDC, and DDR in the development of improved security measures based on operational experience.

X e. Assure that applicable restrictions and instructions are included in procurement requests for incorporation in contractual documents when classified and other specified NSA/CSS information is to be introduced into a contractor's ADP system.

f. Provide the DAA with documentation to support requests for temporary exceptions to specific ADP security measures, including 1) actions to bring the systems into compliance with security requirements; and 2) alternative security measures if appropriate.

X g. Implement the provisions of this regulation within their respective organizations, participate in the NSA/CSS ADP Security Officer Program, and appoint security officers for those ADP systems and networks specified by DDT.

X h. Assist DDC in certifying and DDT in accrediting the security of ADP systems under their operational control.

19. Users of ADP systems will:

X a. Observe the existing rules and regulations governing the secure operation and use of NSA/CSS ADP systems and networks.

b. Assign the security protection mechanisms most appropriate for any permanent data files and programs which they create.

c. Advise the T Operations Watch Center immediately if they suspect that classified data has been misdirected or spilled from ADP systems.

d. Ensure that proper security classification and dissemination markings are contained on machine output.

DOCID: 3978833



## SECTION VI - IMPLEMENTATION

20. This Directive is effective immediately. All regulatory documents and standards implementing the provisions of this Directive shall bear reference to the Directive and copies shall be provided to the ADPL.

B. R. INMAN
Vice Admiral, U. S. Navy
Director, NSA/Chief, CSS

DISTRIBUTION III

DOCID: 3978833

10 JUN 1983

Rec'd P30614 ST

# NATIONAL SECURITY AGENCY
# CENTRAL SECURITY SERVICE

NSA/CSS Directive 10/27
Security Requirements for Automatic Data Processing (ADP) Systems

SECTION


REFERENCES.....I
DEFINITIONS.....II
PURPOSE & APPLICABILITY.....III
POLICY.....IV
SCOPE.....V
RESPONSIBILITIES.....VI
IMPLEMENTATION.....VII


## SECTION I - References

1. References:

a. DoD Directive 5200.28, "Security Requirements for Automatic Data Processing (ADP) Systems," 29 April 1978.

b. "Security Policy on Intelligence Information in Automated Systems and Networks" (C), 4 January 1983, Promulgated by DCI.

c. NSA/CSS Circular , "DoD Computer Security Center Operations," Draft, 21 March 1983.

d. "DoD Trusted Computer System Evaluation Criteria." Final Draft, 27 January 1983.

e. DoD Directive 5215.1, "Computer Security Evaluation Center," 25 October 1982.

f. OMB Circular A-71, Transmittal Memorandum No. 1, "Security of Federal Automated Information Systems," 27 July 1978.

OPI: DCSC (C09 (301) 859-6524)



A9585A.3-79

g. USSID 702, "Automatic Data Processing (ADP) Systems Security," 24 September 1980.

h. NSA/CSS Circular No. 25-5, "Systems Acquisition Management," 2 December 1982.

i. NSA/CSS Regulation 110-2, "The NSA/CSS Automatic Data Processing (ADP) Program," 27 November 1981.

j. NSA/CSS Circular , "Computer Security Vulnerability Reporting Program," TBP.

k. NSA/CSS Directive No. 10-26, "The NSA/CSS Senior Automatic Data Processing Policy Official," 9 December 1980.

l. NSA/CSS Regulation No. 10-35, "Implementation of the Privacy Act of 1974," September 1975.

m. DoD Directive C-5200.5, "Communications Security (COMSEC)," 6 October 1981.

n. DoD Directive 5220.22, "DoD Industrial Security Program," 8 December 1980.

o. NSA/CSS Regulation 60-22, "Industrial Facilities Protection Program," 5 October 1977.

p. NSA/CSS Regulation 90-5, TEMPEST Security Program, 20 August 1980.

## Section II - Definitions

2. The following definitions apply:

a. ADP System Approval - The formal approval by the Designated Approving Authority (DAA) of ADP systems and networks, for the processing, use, storage, and production of material under the jurisdiction of NSA/CSS. The approval is based upon the testing, evaluation, and formal accreditation of the system to verify the application of appropriate security measures to satisfy the requirements contained in the References.

b. Accreditation - The formal declaration that an ADP system or network provides an acceptable level of protection for processing sensitive data in an operational environment. Accreditation is based upon formal certification in accordance with responsibilities assigned under this Directive, criteria contained in the References, and the extent to which the ADP system or network meets these criteria.

c. Certification - The technical evaluation that establishes the extent to which a particular ADP system or network design and implementation meet the requirements prescribed in the References.

d. Communications Security - Protective measures taken to deny unauthorized persons information derived from telecommunications of the United States Government related to national security and to ensure the authenticity of such communications. Such protection results from the application of security measures (including cryptosecurity, transmission security, emissions security) to electrical systems transmitting national security or national security related information. It also includes the application of physical security measures to communications security information or materials.

e. Trusted Computer System - An ADP system that employs sufficient hardware and software integrity measures to allow its use for the simultaneous processing of a designated range of sensitive or classified information.

f. Risk Range - The disparity between the lowest clearance level of users of a system and the classification or compartment/category of the most stringently controlled information processed within a system. As this disparity increases a numerical risk range is produced (e.g., a system with unclassified users which contains SECRET information has a risk range of 3).

g. Level - The steps of increasing trust of individual personnel security clearances and authorizations which includes (1) UNCLASSIFIED, (2) FOUO, (3) CONFIDENTIAL, (4) SECRET, (5) TOP SECRET, and (6) TOP SECRET with full Background Investigation clearances, (7) a single authorization for Compartmented Information (CI) (paragraph h below), and (8) authorization for multiple categories of compartmented information.

h. Compartmented Information (CI) - In addition to the recognized intelligence categories of Category III COMINT, TK and B as defined in Reference b for Sensitive Compartmented Information (SCI), for the purpose of this directive, any information for which the responsible OPI requires a special authorization will be considered a "compartment."

i. Mode of Operation - The degree of trust in HW/SW to enforce the appropriate user access control within a system required by the risk range present.

(1) Multi Level Secure (MLS) - The mode of operation which allows two or more classification levels of information to be processed simultaneously within the same system when some users are not cleared for all levels of information present. The "controlled" (Reference a) mode of operation may be described as a type of Multi Level Security (MLS) where a more limited amount of trust is placed in the HW/SW base of the system.

(2) Compartmented Mode - The mode of operation which allows the system to process two or more types of CI (information requiring a special authorization) or any one type of CI with other than CI, and system access is secured to at least the TOP SECRET level, but all system users need not necessarily be formally authorized access to all types of CI being processed and/or stored in the system.

(3) System High - The mode of operation in which system HW/SW is only trusted to provide need-to-know protection between users. In this mode the entire system, to include all components electrically and/or physically connected, must operate with security measures commensurate with the highest classification and sensitivity of the information being processed and/or stored. All system users in this environment must possess clearances and authorizations for all information contained in the system and all system output must be clearly marked with the highest classification and all system caveats, until manually reviewed by an authorized individual to ensure appropriate classifications and caveats are affixed.

(4) Dedicated Mode - The mode of operation in which the system is specifically and exclusively dedicated to, and controlled for, the processing of that one particular type or classification of information, either for full time operation or for a specified period of time.

j. ADP System - An assembly of computer hardware, firmware and software, which can be used to categorize, sort, calculate, compute, summarize, store, retrieve, control processes and protect data with a minimum of human intervention. This includes those systems where ADP equipments are used in networks and telecommunications systems.

## SECTION III - Purpose and Applicability

3. This directive implements the provisions of References a through g and n as they apply to NSA/CSS, establishes policy for the development and use of trusted computer systems, assigns responsibilities to ensure that NSA/CSS ADP systems and networks and those of its contractors meet computer security requirements. Its provisions are applicable to all NSA/CSS Components, and their contractors, worldwide.

## SECTION IV - Policy

4. All ADP systems under the cognizance of the Director, NSA/Chief, CSS will conform with the computer security specifications contained in the References. These requirements apply to the use of ADP in all telecommunications systems, ADP systems and networks used to store, process, or communicate classified and/or sensitive information, including those equipments in use by NSA/CSS contractors.

5. All NSA/CSS ADP systems will be specified, designed and evaluated to ensure they include the required applicable features of trusted systems which provide the appropriate degree of trust based on Reference d. The degree of trust for HW/SW systems, based on modes of operation, are as follows:

a. Dedicated - Any class of system may be used in Dedicated Mode processing since system trust does not rest on hardware and software protection measures.

b. System High - For systems operating in this mode, Class C2 trusted computer systems are required since the hardware and software protection mechanisms must provide need-to-know access controls.

c. Compartmented - For systems processing more than two comparments (paragraph 2h) of CI or any one compartment of CI with other than CI, Class B2 trusted computer systems must be employed to ensure that trusted labels and sufficient audits are available within the hardware and software to enforce and maintain access controls. All other Compartmented Mode systems may employ Class B1 trusted computer systems.

d. Multi Level - The risk associated with operating Multi Level mode systems need stringent access controls and require the following classes of trusted computer systems based on risk range as defined above (paragraph 2f): Risk ranges of one (1) or two (2) require Class B2 trusted computer systems; a risk range of three (3) requires a Class B3 trusted computer system. Systems with risk ranges in excess of three (3) require Class A1 or more trusted computer systems which will demand careful design, thorough review, and DIRNSA approval.

6. All NSA/CSS ADP Systems and networks in existence prior to the date of this directive must conform with its trusted computer system requirements or have a strategy to meet the trusted computer system requirement for certification and accreditation by 1991.

7. NSA/CSS systems will be connected to ADP systems of another government component, a non-government ADP system, or a contractor facility only after NSA/CSS accreditation to ensure that the inter-connected systems meet NSA/CSS security requirements.

8. Remote terminals and peripheral devices connected to an NSA/CSS telecommunications or ADP system will be considered part of the system. In order to ensure that NSA/CSS security requirements are met, a technical evaluation and formal certification must be provided, attesting that the terminals and devices, and the areas in which they are located, meet NSA/CSS security requirements. When such terminals and devices are connected to more than one NSA/CSS ADP system, the security requirements highest among the associated systems must be met. If the various components of the connected systems cannot all meet the most stringent security requirements for each of the systems, the connected system must be certifiable and accredited as either a compartmented or multi-level system, as appropriate.

DOCID: 3978833

## SECTION V - Scope

9. This Directive encompasses all ADP systems and networks operated by NSA/CSS and their contractors. This includes all connections of NSA/CSS systems to other government computer systems and the provision of NSA system remote terminals to other government agencies.

10. Cryptologic information in systems operated by non-NSA/CSS components or contractors shall be protected IAW References a, b, g and n as applicable.

## SECTION VI - Responsibilities

11. Under the provisions of References a and b, the Director, NSA/Chief, CSS (or, in his absence, the Deputy Director, NSA) is the Designated Approving Authority (DAA) for any NSA/CSS or NSA/CSS contractor ADP system or network processing classified and/or sensitive information. The Deputy Director, NSA, is authorized to act as the DAA for NSA/CSS ADP systems or networks not operating in the compartmented or multi level-secure mode.

a. The DAA will approve all NSA/CSS ADP systems or networks for the processing, use, storage, and production of classified and/or sensitive information.

b. The DAA will authorize temporary exceptions of up to one year to specific ADP security measures that would impair operation and mission effectiveness, provided that continuous progress is made toward ultimate compliance.

c. On an annual basis, the Director, NSA/Chief, CSS will assess the progress toward employing trusted computer systems and networks within NSA/CSS.

12. The Deputy Director for Telecommunications and Computer Services (DDT), (designated separately as the Senior ADP Policy Official (SADPPO) IAW Reference k.) will:

a. Using the recommendations of system certifiers, accredit the operation of all NSA/CSS and NSA/CSS contractor ADP systems and networks for the processing, use, storage, and production of classified and/or sensitive information.

b. Assure that NSA/CSS ADP systems and networks, and those of its contractors continuously meet the security of Section IV, Policy, above and that continued approval of each system is based upon the results of a recurring review, testing, system configuration control, and favorable evaluation of system security features required by the class of system (Reference d) used in a specific operational environment and those other factors required by the certification/accreditation process.

c. Control and administer the NSA/CSS ADP Security Officer Program.

d. Approve the adequacy of plans for the security of each NSA/CSS ADP system or network being developed, procured, or operated.

e. Develop an NSA/CSS reporting system (paragraph 11c, above) to provide the Director, NSA/Chief, CSS with basic data on the status of the security of NSA/CSS ADP systems, including mode of operation, range of information and users of the system, trusted evaluation class used and required, problems and corrective actions needed or in process, as well as an inventory of ADP terminals available for each TEMPEST control zone.

f. Approve the connection of other U.S. Government component or contractor ADP systems to NSA/CSS ADP systems and networks based on evaluations of the external systems by Director DoD CSC, DDA, and DDC.

g. Ensure that the Computer Security Vulnerability Reporting Program (Reference j) is implemented through the ADP Security Officer Program.

h. Act as the central NSA/CSS focal point per Reference e to the DoD CSC for the evaluation of trusted computer systems within NSA/CSS.

13. The Deputy Director for Communications Security (DDC) will:

a. Certify, in the formal accreditation process, that ADP systems under the authority of NSA/CSS have satisfied minimum COMSEC and TEMPEST requirements prescribed in References m and p.

b. Evaluate and approve cryptography to be used in NSA/CSS ADP systems.

c. Provide COMSEC assistance in support of effective ADP security to other U.S. Government components, upon request.

14. The Director, DoD CSC, as the principal technical advisor to the Director, NSA/Chief CSS on computer security will:

a. Publish and maintain trusted computer system standards and criteria IAW Reference c.

b. Advise the NSA/CSS components and their contractors on the application of Reference d in meeting computer security requirements.

c. Assist the NSA/CSS components in carrying out their computer security requirements for all ADP systems and networks developed IAW References h and i.

d. Certify to DDT and the NSA OPI for the data processed, the extent to which operational systems, planned expansions or connections to external ADP systems and networks at NSA, field locations and contractor installations meet computer security requirements IAW References a, b, c, g, and o, and employ the appropriate trusted computer system in the processing of classified and/or sensitive information.

e. Certify to DDT the extent to which ADP systems and networks of other government components or contractors, which are to be connected to NSA/CSS systems or networks, meet the same evaluation criteria (Reference d) required for the NSA/CSS system or network.

f. Develop trusted computer systems for use with cryptographic devices employed in networks and other computer applications.

15. The Deputy Director for Administration (DDA) will:

a. Establish and promulgate physical and personnel security standards necessary to provide adequate safeguards and controls for access to NSA/CSS and NSA/CSS Contractor ADP areas, network areas, telecommunications areas, and terminal areas.

b. Certify to DDT that telecommunications, ADP and network facilities of both NSA/CSS and its contractors meet current physical security standards.

c. Certify to DDT that telecommunications, ADP, and network facilities of other government components or contractors, which are to be connected to NSA/CSS ADP systems or networks, meet current physical security standards.

16. The Deputy Director for Plans and Resources (DDPR) will secure General Accounting Office approval for all procedures affecting NSA/CSS ADP systems that process fiscal and accounting data, and will advise DDT that approval has been received.

17. The Assistant Director for Installation and Logistics (ADIL) is responsible for acting as the Agency point of contact on matters relating to the Defense Industrial Facilities Protection Program IAW Reference o.

18. The Chiefs of the Key Components and the Chiefs of the Field Components who develop, manage, operate, or are otherwise responsible for ADP systems, networks, and/or telecommunications systems will:

a. Assure that ADP systems and networks to be developed, procured, or leased meet the requirements of this directive to provide adequate security safeguards for classified and/or sensitive information contained in the system.

b. Implement the provisions of this Directive within their respective organizations, participate in the NSA/CSS ADP Security Officer Program, and appoint security officers for those telecommunications systems, ADP systems, and networks under their cognizance.

c. Establish standards for the protection of information under their control and certify to DDT that these standards have been met and this information can be processed and or stored on the telecommunication system, ADP system or network being accredited.

d. Specify each type of Compartmented Information (paragraph 2h) which needs protection through the use of special authorizations and caveats (labels) thereby ensuring that all data sets/bases are properly secured through the use of the appropriate trusted computer system, and ensure a distinct internal label (reference d) is assigned to each level (paragraph 2g) of information processed.

e. Assure that those telecommunications systems, ADP systems, and networks designed for future placement and those systems already installed conform to the security requirements of this Directive and, if not, bring them into compliance with the standards prescribed at the earliest possible date.

f. Support requests to the DAA for temporary exceptions to specific ADP security measures, including (1) actions to bring the system into compliance with security requirements; (2) alternative security measures, if appropriate.

g. Protect privacy information or any other data with restricted dissemination caveats with the same trusted computer system requirements used for compartmented information (CI).

19. The Users of NSA/CSS telecommunications systems, ADP systems, and networks will:

a. Observe the existing rules and regulations governing the secure operation and use of NSA/CSS telecommunications systems, ADP systems, and networks.

b. Employ the security protection capabilities provided by the system for all data files and other information which they create or use.

c. Advise the T Operations Watch Center immediately if they suspect that classified data has been misdirected or spilled from ADP systems.

d. Report flaws in security controls to their designated Computer Equipment Systems Security Officer (CESSO).

e. Ensure that proper security classification and dissemination markings are contained on machine output.

f. Perform a content review of all output generated from a System High system, to assure that the appropriate classification has been assigned prior to releasing the output to personnel who do not have access to all the information in the system, or prior to assigning a lower classification to that output.

DOCID: 3978833

## SECTION VII - Implementation

20. This directive is effective immediately.

LINCOLN D. FAURER
Lieutenant General, USAF
Director, NSA/Chief, CSS

DISTRIBUTION III

DOCID: 3978833

[redacted] P.L. 86-36

# NATIONAL SECURITY AGENCY
# CENTRAL SECURITY SERVICE
FORT GEORGE G. MEADE, MARYLAND

NSA/CSS DIR. NO. *10-27
DATE: 29 March 1984

# NSA/CSS DIRECTIVE

## SECURITY REQUIREMENTS FOR AUTOMATIC DATA PROCESSING (ADP) SYSTEMS

SECTION

REFERENCES..... I
PURPOSE & APPLICABILITY..... II
DEFINITIONS.....III
POLICY..... IV
SCOPE..... V
RESPONSIBILITIES..... VI

## SECTION I - REFERENCES

1. References:

a. DoD Directive 5200.28, "Security Requirements for Automatic Data Processing (ADP) Systems," 18 December 1972, with changes.

b. DCI Publication, "Security Policy on Intelligence Information in Automated Systems and Networks," 4 January 1983, and its attachment, "Computer Security Manual."

c. NSA/CSS Directive 21-1, "DoD Computer Security Center Operation," dated 29 March 1984.

d. "DoD Trusted Computer System Evaluation Criteria," 15 August 1983.

e. DoD Directive 5215.1, "Computer Security Evaluation Center," 25 October 1982.

*This Directive supersedes NSA/CSS Directive Number 10-27, dated 30 November 1979.

OPI: DDPP [redacted] P.L. 86-36

A9585D.3-73

DOCID: 3978833



f. OMB Circular A-71, Transmittal Memorandum No. 1, "Security of Federal Automated Information Systems," 27 July 1978.

g. DoD Directive 5220.22, "DoD Industrial Security Program," 8 December 1980.

h. NSA/CSS Circular No. 25-5, "System Acquisition Management," 2 December 1982.

i. NSA/CSS Regulation 110-2, "The NSA/CSS Automatic Data Processing (ADP) Program," 27 November 1981.

j. NSA/CSS Directive No. 10-26, "The NSA/CSS Senior Automatic Data Processing Policy Official," 9 December 1980.

k. NSA/CSS Regulation No. 10-35, "Implementation of the Privacy Act of 1974," 22 June 1983.

l. DoD Directive C-5200.5, "Communications Security (COMSEC)," 6 October 1981.

m. NSA/CSS Regulation 60-22, "Industrial Facilities Protection Program," 5 October 1977.

n. NSA/CSS Regulation 90-5, "TEMPEST Security Program," 20 August 1980.

o. NSA/CSS Manual 90-4, "ADP Security Design and Operating Standards," 4 January 1980.

## SECTION II - PURPOSE AND APPLICABILITY

2. This Directive implements the provisions of the references as they apply to NSA/CSS and the SCE's; establishes policy for NSA/CSS, and the SCE's for the development or selection and use of trusted computer systems, and assigns responsibilities to ensure that NSA/CSS and SCE ADP systems and those of their contractors meet computer security requirements. The provisions of this Directive apply to all NSA/CSS and SCE Components, its contractors and affiliates worldwide.

## SECTION III - DEFINITIONS

3. The following definitions apply:

a. ADP System - An assembly of Computer Hardware (HW), Firmware (FW) and Software (SW), which can be used to categorize, sort, calculate, compute, summarize, store, retrieve, control, process and protect data with a minimum of human intervention.

DOCID: 3978833



b. Certification - The act of confirming that a technical evaluation has been performed in sufficient depth to assure that a particular ADP system or network design meets or exceeds the requirements stated in the references.

c. Accreditation - The formal declaration that an ADP system provides an acceptable level of protection for processing sensitive data in an operational environment. Accreditation is based upon technical evaluation, risk assessment, cost benefit analysis, operational requirements and the meeting of prescribed standards.

d. ADP System Approval - The formal approval by the Designated Approving Authority (DAA) of ADP Systems for processing, use, storage, and production of material under the jurisdiction of NSA/CSS. This approval is granted after testing, evaluation, certification and formal accreditation.

e. Communications Security - Protective measures taken to deny unauthorized persons information derived from telecommunications of the United States Government related to national security and to ensure the authenticity of such communications. Such protection results from the application of security measures (including cryptosecurity (transmission security, and emissions security) to electrical systems generating, handling, processing, or using national security or national security related information. It also includes the application of physical security measures to communications security information or materials.

f. Compartmented Information (CI) - In addition to the recognized national level compartments of SCI, for the purpose of this Directive, any information for which the owner requires a special access authorization may be considered a "sub-compartment." Specific added security measures or handling instructions may be applied on a case-by-case basis for classes or sets of information determined to be sensitive.

g. Level - The steps of increasing trust of individual personnel security clearances and authorizations which includes (1) UNCLASSIFIED, (2) FOUO, (3) CONFIDENTIAL, (4) SECRET, (5) TOP SECRET and, (6) TOP SECRET with full Background Investigation clearances, (7) a single authorization for Compartmented Information (CI) (Paragraph h below), and (8) authorization for multiple categories of compartmented information.

h. Mode of Operation - The degree of trust in HW/SW to enforce the appropriate user access control within a system required by the risk range present.

(1) Multi-Level Secure (MLS) - The mode of operation which allows two or more classification levels of information to be processed simultaneously within the same

DOCID: 3978833



system when some users are not cleared for all levels of information present. The "controlled" (Reference a) mode of operation may be described as a type of Multi-Level Security (MLS) where a more limited amount of trust is placed in the HW/SW base of the system.

The Director, NSA/CSS, has determined the need to support Multi-Level Mode Operations in addition to the three specified modes contained in the DCI Policy. In the Multi-Level Mode, the technical security requirements for each configuration will be specified on a case-by-case basis.

(2) Compartmented Mode - The mode of operations which allows computer systems to process two or more types of Sensitive Compartmented Information (SCI) concurrently. All systems users need not be cleared for all types of SCI processed, but must be fully cleared for at least one type of SCI for unescorted access to the computer. Certain formal access programs or SCI subcompartments, agreed upon by the appropriate Key Component, may require added computer security features or procedures.

(3) System High - The mode of operation in which system HW/SW is only trusted to provide need-to-know protection between users. In this mode, the entire system (to include all components electrically and/or physically connected) must operate with security measures commensurate with the highest classification and sensitivity of the information being internally processed or stored. All system users in this environment must possess clearances and authorizations for all information contained in the system.

(4) Dedicated Mode - The mode of operation in which the system is specifically and exclusively dedicated to, and controlled for, the processing of one particular type or classification of information, either full time or for a specified duration.

i. Risk Level - The disparity between the lowest clearance level of users of a system and the classification or compartment/category of the most stringently controlled information processed within a system. As this disparity increases, a numerical risk range is produced (e.g., a system with unclassified users which contain SECRET information has a risk range of 3).

j. Trusted Computer System - An ADP system that employs sufficient hardware and software integrity measures to allow its use for the simultaneous processing of a range of sensitive or classified information.

DOCID: 3978833



SECTION IV - POLICY

4. All ADP systems under the cognizance of the Director, NSA/Chief, CSS, will conform with the computer security specification contained in the references. These requirements apply to all NSA/CSS ADP systems and those of its affiliated contractors that are used to store, process or communicate classified and/or sensitive information.

5. All NSA/CSS ADP systems will be specified, designed and evaluated to ensure they include the required applicable features of trusted systems. The individuals responsible for certifying NSA/CSS systems will determine the degree of assurance needed to sufficiently safeguard the system based on the intended application. The degree of trust for HW/SW systems, based on the modes of operation, are specified below. The structure of the criteria and classes of trusted systems are contained in Reference d.

a. Dedicated - Any class of system may be used in Dedicated Mode processing since system trust does not rest on hardware and software protection measures.

b. System High - For systems operating in this mode, Class C2 trusted computer systems are required since the hardware and software protection mechanisms must provide need-to-know access controls. The system output data must be clearly marked with the appropriate classification and caveats as determined by content. The data will then be manually reviewed by an authorized individual to ensure the appropriate classifications and caveats are affixed.

c. Compartmented - For systems processing more than two compartments (Paragraph 2h) of CI or any one compartment of CI with other than CI, Class B2 trusted computer systems must be employed to ensure that trusted labels and sufficient audits are available within the hardware and software to enforce and maintain access controls. All other Compartmented Mode systems may employ Class B1 trusted computer systems.

d. Multi-Level - The risk associated with operating Multi Level mode systems need stringent access controls and require the following classes of trusted computer systems based on risk ranges as follows: Risk ranges of one (1) or two (2) require Class B2 trusted computer systems; a risk range of three (3) requires a Class B3 trusted computer system. Systems with risk ranges in excess of three (3) require Class A1 or more trusted computer systems.

6. All NSA/CSS ADP systems in existence on the date of this Directive must conform with its trusted computer system requirements, or a strategy must be developed by the responsible element to

DOCID: 3978833



meet the requirements for certification and accreditation. Strategy planning will be started not later than six months after publication of this Directive.

7. NSA/CSS Systems will be connected to ADP systems of another government component, a non-government ADP system, or a contractor facility only after NSA/CSS accreditation to ensure that the interconnected systems meet NSA/CSS security requirements.

8. With the advent of powerful personal computers and the increasing demand for these devices by the workforce, such remote terminals and their peripheral devices (when connected to an NSA/CSS ADP system) will be considered as an integral part of that system. Thus, to confirm that NSA/CSS security requirements are met, a technical evaluation and formal certification must be provided, attesting that the equipments and physical environment meet the requisite security standards. Certification and accreditation will be established at the highest level of classified information to be processed.

## SECTION V - SCOPE

9. This Directive encompasses all ADP systems operated by NSA/CSS and its contractors. This includes all connections of NSA/CSS systems to other government computer systems and the provision of NSA system remote terminals to other government agencies.

10. Cryptologic information in systems operated by non-NSA/CSS components or contractors shall be protected in accordance with References a, b and g where applicable.

## SECTION VI - RESPONSIBILITIES

11. Under the provisions of References a and b, the Director, NSA/Chief, CSS (or, in his absence, the Deputy Director, NSA), is the Designated Approving Authority (DAA) for any NSA/CSS or NSA/CSS contractor ADP systems processing classified and/or sensitive information. The Deputy Director, NSA, is authorized to act as the DAA for NSA/CSS ADP systems not operating in the compartmented or multi-level-secure mode.

a. The DAA will approve all NSA/CSS ADP systems or networks for the processing, use, storage, and production of classified and/or sensitive information.

b. The DAA will authorize temporary exceptions of up to one year to specific ADP security measures that would impair operation and mission effectiveness, provided that continuous progress is made toward ultimate compliance. The DAA will authorize

DOCID: 3978833



exceptions for a period in excess of one year, if appropriate, in support of Research and Engineering on ADP systems.

12. The Deputy Director for Plans and Policy (DDPP) will:

a. Monitor the implementation of National, Departmental and Agency policy relative to ADP Security, assuring that due cognizance of responsibilities are maintained with Signals Intelligence and Communications Security policy.

b. Insure strict compliance with National, Departmental and Agency regulations relative to the release of classified and unclassified information as pertains to the NSA/CSS Information Security Program.

c. Monitor new and on-going ADP Security programs as they relate to foreign governments or foreign citizens, ensuring that established relationships are not jeopardized or extended beyond the intent of legal agreements.

d. In concert with the Director, Computer Security Center, assist in the evaluation and propriety of all requests of the Center relative to Technology Transfer.

e. Review all proposed releases of information to conferences, symposia, etc., or to the press.

13. The Deputy Director for Telecommunications and Computer Services (DDT), designated separately as the Senior ADP Policy Official (SADPPO) in accordance with Reference j, will:

a. Accredit the operations of all NSA/CSS, SCE, and NSA/CSS affiliated contractor ADP systems, for the processing, use, storage and production of classified or sensitive information. Systems security standards apply only to contractor owned/operated ADP systems which are employed in support of NSA/CSS.

b. Assure that NSA/CSS ADP systems and those of its affiliated contractors continuously meet the security of Section IV, Policy, above and that continued approval of each system is based upon the results of a recurring review, testing, system configuration control, and favorable evaluation of system security features required by the class of system (Reference d) used in a specific operational environment and those other factors required by the certification/accreditation process.

c. Control and administer the NSA/CSS ADP Security Officer Program.

d. Approve the adequacy of plans for the security of each NSA/CSS ADP system being developed, procured, or operated.

DOCID: 3978833



e. Maintain a current data base on the status of the security of NSA/CSS ADP systems including problems/corrective actions required or in process, as well as an inventory of ADP terminals available for each control zone.

f. Approve the connection of other U.S. Government components or contractor ADP systems to NSA/CSS ADP systems after considering the evaluations of the external systems by Director DOD CSC, DDA, and DDC.

g. Ensure that the Computer Security Vulnerability Reporting Program is implemented through the ADP Security Officer Program.

h. Act as the central NSA/CSS focal point per Reference e to the DoD CSC for the evaluation of trusted computer systems within NSA/CSS.

14. The Deputy Director for Communications Security (DDC) will:

a. Establish minimum COMSEC and TEMPEST requirements for NSA/CSS ADP systems and certify, in the formal accreditation process, that ADP systems under the authority of NSA/CSS have satisfied minimum COMSEC and TEMPEST requirements.

b. Evaluate and approve communication security measures and cryptography to be used in ADP systems, and in any networks in which they participate.

c. Provide COMSEC assistance in support of effective ADP security to other U.S. Government components, upon request.

d. Certify to DDT the extent to which ADP networks of other Government components or contractors, that are to be connected to NSA/CSS networks, meet the minimum COMSEC criteria required for the NSA/CSS network. Systems security standards apply only to contractor owned/operated ADP systems which are employed in support of NSA/CSS.

15. The Director, DoD Computer Security Center (CSC), as the principal technical advisor to the Director, NSA/Chief, CSS on computer security will:

a. Publish and maintain trusted computer system standards and criteria as prescribed in Reference d.

b. Advise and assist the NSA/CSS components and their contractors on the application of Reference d in meeting computer security requirements.

c. Assist the NSA/CSS components in carrying out their computer security requirements for all ADP systems developed according to Reference h and i.

DOCID: 3978833



d. Certify to DDT and provide notification to the NSA Office of Primary Interest for the data processed, the extent to which operational systems, planned expansions or connections to external ADP systems/networks at NSA, field locations, and contractor installations meet computer security requirements.

e. Provide technical evaluation services to the DIRNSA and DDT for purposes of accrediting the operation of NSA/CSS and contractor computer systems and any networks in which they participate.

f. Periodically distribute, when received, additions to the Evaluated Products List of commercially available hardware and software products that can be safely used to protect sensitive data in computer systems as prescribed by Paragraph 5.

g. Publish a variety of publications to users, operators, and managers of computer systems on the secure use and operations of NSA/CSS systems.

h. Annually, the Director, Computer Security Center will report to the Director, NSA/CSS, his assessment of the progress toward employing trusted computer systems within the cognizance of NSA/CSS, in accordance with the terms of this Directive.

16. The Deputy Director for Administration (DDA) will:

a. Establish and promulgate physical and personnel security standards necessary to provide adequate safeguards and controls for access to NSA/CSS and NSA/CSS Contractor ADP areas, network areas, telecommunication areas, and terminal areas.

b. Certify to DDT that ADP and network facilities of both NSA/CSS and its contractors meet physical security standards.

c. Certify to DDT that ADP and network facilities of other government components or contractors, which are to be connected to NSA/CSS ADP systems or networks, meet physical security standards.

17. The Deputy Director for Plans and Resources (DDPR) will secure General Accounting Office approval for all procedures affecting NSA/CSS ADP systems that process fiscal and accounting data, and will advise DDT that approval has been received. Additionally, the A/DDPR is designated separately as the alternate Senior ADP Policy Official (SADPPO).

DOCID: 3978833



18. The Assistant Director for Installation and Logistics (ADIL) is responsible for acting as the Agency point of contact on matters relating to the Defense Industrial Facilities Protection Program in accordance with Reference m.

19. The Chiefs of the Key Components and the Chiefs of the Field Components who develop, manage, operate, or are otherwise responsible for ADP systems and networks will:

a. Assure that ADP systems and networks to be developed, procured, or leased meet the requirements of this Directive to provide adequate security safeguards for classified and/or sensitive information contained in the system.

b. Implement the provisions of this Directive within their respective organizations, participate in the NSA/CSS ADP Security Officer Program, and appoint security officers for those telecommunications systems, ADP systems, and networks under their cognizance.

c. Establish standards for the protection of information under their control and certify to DDT that these standards have been met and this information can be processed and or stored on the ADP system or network being accredited by making maximum use of DoD Computer Center Standards.

d. Identify that classified information which required additional special protection as Compartmented Information which needs protection by means of special authorizations and caveats.

e. Assure that those ADP systems, designed for future placement and those systems already installed conform to the security requirements of this Directive and, if not, bring them into compliance with the standards prescribed at the earliest possible date.

f. Support requests to the DAA for temporary exceptions to specific ADP security measures, including (1) actions to bring the system into compliance with security requirements; (2) alternative security measures, if appropriate.

g. Protect privacy information, protected company proprietary information, or any other data with restricted dissemination caveats with the same trusted computer system requirements used for compartmented information (CI).

20. The Users of NSA/CSS ADP systems will:

a. Observe the existing rules and regulations governing the secure operation and use of NSA/CSS ADP systems and networks.

DOCID: 3978833



b. Employ the security protection capabilities provided by the system for all data files and other information which they create or use.

c. Advise the T Operations Watch Center immediately if they suspect that classified data has been misdirected or spilled from ADP systems.

d. Report flaws in security controls to their designated Computer Equipment Systems Security Officer (CESSO).

e. Ensure that proper security classification and dissemination markings are contained on machine output.

f. Perform a content review of all output generated from a System High system, to assure that the appropriate classification has been assigned prior to releasing the output to personnel who do not have access to all the information in the system, or prior to assigning a lower classification to that output.

LINCOLN D. FAURER
Lieutenant General, USAF
Director, NSA/Chief, CSS

DISTRIBUTION III
PLUS: L22 (10% Stock)