APPENDIX V

PROTECTION OF INFORMATION HANDLED IN IT AND COMMUNICATION SYSTEMS

MULTINATIONAL INDUSTRIAL SECURITY WORKING GROUP
MISWG Document Number 13 **25 June 1993**
(Amended 5 September 2002)

PROTECTION OF INFORMATION HANDLED IN IT AND COMMUNICATION SYSTEMS

CHAPTER I

INTRODUCTION

GENERAL ASPECTS

1. This document has been approved by the Multinational Industrial Security Working Group (MISWG). The requirements contained in this document provide guidance for contracts. The document can be added as a reference to contracts or Project Security Instructions (PSI) where applicable.

2. The security policy and requirements in this document shall apply to all communications and information systems and networks (hereinafter SYSTEMS) handling classified information.

3. SYSTEMS handling RESTRICTED information require security measures to protect the confidentiality of that information.

1. SYSTEMS handling CONFIDENTIAL information and above require security measures to protect confidentiality, integrity and availability of the information they contain. The security measures needed to meet requirements as laid down in this document will be determined by the designated Security Accreditation Authority (SAA) and will be commensurate with the assessed risk and consistent with the policy stated in this document.

THREATS TO AND VULNERABILITIES OF SYSTEMS

5. In general terms, a threat can be defined as a potential for the accidental or deliberate compromise of security. In the case of SYSTEMS, such a compromise involves loss of one or more of the properties of confidentiality, of integrity and of availability. A vulnerability can be defined as a potential weakness or lack of controls that would facilitate or allow a threat actuation against a specific asset or target. A vulnerability may be an omission or it may relate to a deficiency in a control's strength, completeness or consistency; it may be technical, procedural or operational in nature.

SECURITY MEASURES

6. The main purpose of the security measures stated in this document is to provide requirements for protection against unauthorised disclosure of information (the loss of confidentiality). Loss of integrity and

availability of information is in this context regarded as important only as far as this, in turn, would lead to loss of confidentiality.

SYSTEM-SPECIFIC SECURITY REQUIREMENT STATEMENT (SSRS)

7. For all SYSTEMS handling classified information, a SYSTEM-Specific Security Requirement Statement (SSRS) shall be required to be produced by the System Operational Authority (SOA) in co-operation with input and assistance as required from the project staff and INFOSEC Authority, and approved by the SAA.

8. The SSRS shall form the binding agreement between the System operational authority and the SAA against which the SYSTEM is to be accredited.

9. All SYSTEMS handling classified information shall be accredited.

CHAPTER II

SECURITY RESPONSIBILITIES

SECURITY ACCREDITATION AUTHORITY (SAA)

10. The SAA shall be either:

- a National Security Authority (NSA),
- a Designated Security Authority (DSA). This authority is designated by the Member States depending on the SYSTEM to be accredited.

11. The SAA shall be responsible for ensuring the compliance of SYSTEMS with security policy. One of its tasks shall be to grant the approval of a SYSTEM to handle classified information to a defined level of classification in its operational environment.

SYSTEM OPERATIONAL AUTHORITY (SOA)

12. An SOA shall be responsible for the implementation and operation of controls and special security features for each SYSTEM. This responsibility shall extend throughout the life cycle of the SYSTEM from the project concept stage to final disposal.

13. The SOA shall be responsible for all security measures designed as part of the SYSTEM. This responsibility includes the preparation of the SSRS and the Security Operating Procedures (SecOPs).

14. The SOA may delegate a part of its responsibilities where appropriate to, for instance the INFOSEC security officer and the INFOSEC site security officer. The various INFOSEC functions may be performed by a single person.

INFOSEC AUTHORITY (IA)

15. The SOA can appoint an INFOSEC Authority (IA) to assist in daily business. The IA will act as direct representative of the SAA. As a minimum the IA will be responsible for the following INFOSEC office activities:

- providing technical advice and assistance to the SAA
- assisting in the development of the SSRS
- reviewing the SSRS to ensure consistency with the present Council Security Regulations and the INFOSEC policies and architecture documents
- participating in the accreditation panels/boards as required and providing INFOSEC recommendation on accreditation to the SAA
- providing support to the INFOSEC training and education activities
- providing technical advice in investigation of INFOSEC related incidents
- establish technical policy guidance to ensure that only authorised software is used.

USERS

16. All users shall be responsible for ensuring that their actions do not adversely affect the security of the SYSTEM that they are using. Furthermore users are required to report unusual incidents or prospective vulnerabilities to the IT SOA.

INFOSEC TRAINING

17. INFOSEC education and training shall be available at various levels, and for various personnel, as appropriate.

CHAPTER III

NON-TECHNICAL SECURITY MEASURES

PERSONNEL SECURITY

18. Users of the SYSTEM shall be cleared and have a need-to-know, as appropriate for the classification and content of the information handled within their particular SYSTEM. Access to certain equipment (e.g. cryptographic) or information specific to security of SYSTEMS will call for special clearance issued by the relevant NSA/DSA.

19. The SAA shall designate all sensitive positions and specify the level of clearance and supervision required by all personnel occupying them.

20. In general, as far as possible, SYSTEMS shall be specified and designed in a way that facilitates the allocation of duties and responsibilities to personnel. The intend is to prevent one person having complete knowledge or control of the system security keys points. The aim should be that collusion between two or more individuals would be necessary for alteration or intentional degradation of the system or network to take place. This can be achieved applying procedural measures. For SYSTEMS intended for processing SECRET and higher information or systems processing SPECIAL CATEGORY information, it will be mandatory to have such procedures in place.

PHYSICAL SECURITY

21. IT and Remote Terminal/Workstation Areas in which classified information is handled by IT means, or where potential access to such information is possible, shall be established in a secure area approved by the appropriate security authority.

CONTROL OF ACCESS TO A SYSTEM

22. All information and material which allow access control to a SYSTEM shall be protected under arrangements commensurate with the highest classification and the category designation of the information to which it may give access.

CHAPTER IV

TECHNICAL SECURITY MEASURES

SECURITY OF INFORMATION

23. It shall be incumbent upon the originator of the information to identify and classify all information-bearing documents, whether they are in the form of hard-copy output or computer storage media. Each page of hard-copy output shall be marked, at the top and bottom, with the classification. Output, whether it is the form of hard-copy or computer storage media shall have the same classification as the highest classification of the information used for its production. The way in which a SYSTEM is operated may also impact on the classification of outputs of that system.

24. It shall be incumbent upon an organisation and its information holders to consider the problems of aggregation of individual elements of information, and the inferences that can be gained from the related elements, and determine whether or not a higher classification is appropriate to the totality of the information.

25. The fact that the information may be a brevity code, transmission code or in any form of binary representation does not provide any security protection and should not, therefore, influence the classification of the information.

26. When information is transferred from one SYSTEM to another the information shall be protected during transfer and in the receiving SYSTEM in the manner commensurate with the original classification and category of the information.

27. All computer storage media shall be handled in a manner commensurate with the highest classification of the stored information or the classification identified on the media label, and at all times shall be appropriately protected.

28. Re-usable computer storage media used for recording classified information shall retain the highest classification for which they have ever been used until that information has been properly downgraded or declassified and the media reclassified accordingly, or the media declassified or destroyed by an approved national procedure.

CONTROL AND ACCOUNTABILITY OF INFORMATION

29. The SYSTEM shall have an automated and / or manual mechanism to enable investigation of system and user activity. This mechanism will provide logging information with the possibility to indicate user or system identification, date and time of activity and executed activity. Depending on the level of classification of the SYSTEM, following activities will be logged:

ALL CLASSIFICATION LEVELS	access to the SYSTEM and activities to alter user rights including unsuccessful attempts
CONFIDENTIAL and above	access to classified information (files)
SECRET and above	alterations to content of classified information (files).

30. Access and manipulation related data shall be retained for 18 months as a minimum. After that time they will be destroyed in accordance with national rules for the classification of the system.

31. Classified outputs held within the secure area may be handled as one classified item and need not be registered, provided the material is identified, marked with its classification and controlled in an appropriate manner.

32. Where output is generated from a SYSTEM handling classified information, and transmitted to a remote terminal/workstation area from an IT area, procedures, agreed by the SAA shall be established for controlling the remote output. For SECRET and above, such procedures shall include specific instructions for accountability of the information.

HANDLING AND CONTROL OF REMOVABLE COMPUTER STORAGE MEDIA

33. All classified removable computer storage media shall be handled as classified material. Appropriate identification and classification markings need to be adapted to the specific physical appearances of the media, to enable it to be clearly recognised.

34. Users shall take the responsibility for ensuring that classified information is stored on media with the appropriate classification marking and protection. Procedures shall be established to ensure that, for all levels of information, the storage of information on computer storage media is being carried out in accordance with the security regulations.

DECLASSIFICATION AND DESTRUCTION OF COMPUTER STORAGE MEDIA

35. Computer storage media used for recording classified information may be downgraded or declassified if approved by appropriate security authority and/or national procedures are applied.

36. Computer storage media, which has held TOP SECRET or special category information, shall not be declassified and reused.

37. If computer storage media cannot be declassified or is not reusable, it shall be destroyed by a procedure approved by the SAA.

COMMUNICATIONS SECURITY

38. When classified information is transmitted electromagnetically, special measures shall be implemented to protect the confidentiality of such transmissions. The appropriate security authority shall determine the requirements for protecting transmissions from detection, interception or exploitation. The information being transmitted in a communication system shall be protected based upon the requirements for confidentiality.

39. Classified information shall not be transmitted in clear text. Only cryptographic systems approved by the NSA/DSA concerned shall be used for the encryption of classified information, irrespective of the method of transmission.

40. However, under exceptional circumstances, information classified RESTRICTED, CONFIDENTIAL and SECRET may be transmitted in clear text provided each occasion is explicitly authorised by the relevant NSA/DSA.

INSTALLATION AND EMISSION SECURITY

41. All equipment shall be installed in accordance with current national security policy.

42. Security measures shall be implemented to protect against the compromise of classified information through unintentional electromagnetic emissions. The measures shall be commensurate with the risk of exploitation and the sensitivity of the information.

CHAPTER V

SECURITY DURING HANDLING

SECURITY OPERATING PROCEDURES

43. Security Operating Procedures (SecOPs) define the principles to be adopted on security matters, the operating procedures to be followed, and personnel responsibilities. The SecOPs shall be prepared under the responsibility of the System Operational Authority.

SOFTWARE PROTECTION/CONFIGURATION MANAGEMENT

44. The software versions in use should be verified at regular intervals to ensure their integrity and correct functioning.

45. New or modified versions of software should not be used for the handling of classified information until authorised by the System Operational Authority.

CHECKING FOR THE PRESENCE OF MALICIOUS SOFTWARE/COMPUTER VIRUSES

46. Checking for the presence of malicious software/computer viruses shall be periodically carried out in accordance with the requirements of the SAA.

47. All computer storage media should be checked for the presence of any malicious software or computer viruses, before being introduced to any SYSTEM.

MAINTENANCE

48. Contracts and procedures for scheduled and on-call maintenance of SYSTEMS for which a SSRS has been produced shall specify requirements and arrangements for maintenance personnel and their associated equipment entering an IT area.

49. The requirements shall be clearly stated in the SSRS and the procedures shall be clearly stated in the SecOPs. Contractor maintenance requiring remote access diagnostic procedures shall be permitted only in exceptional circumstances, under stringent security control, and only with the approval of the SAA

SECURITY ADMINISTRATION

50. The security settings of SYSTEMS shall only be changed with approval of the SOA. For SYSTEMS intended for processing SECRET or higher information or for systems processing SPECIAL CATEGORY information, it will be mandatory to have written approval of the SOA prior to making such changes.

51. Alterations to security settings of SYSTEMS shall be reviewed by the SOA using log file information.

CHAPTER VI

ACCREDITATION

INTRODUCTION

52. All SYSTEMS handling information classified CONFIDENTIAL and above shall be accredited prior to processing such information. Accreditation is the authorisation and approval granted to a SYSTEM to process classified information in its specified operational environment. Such accreditation should be made after all appropriate security procedures have been implemented and a sufficient level of protection of the system resources has been achieved.

53. The SAA will base accreditation upon information provided in the SSRS, Security Operating Procedures (SecOPs) and any other relevant documentation. Sub-systems and remote terminals/workstations shall be accredited as part of all SYSTEMS to which they are connected. Where a SYSTEM supports other organisations, the relevant Security Authorities shall mutually agree on the accreditation.

54. The accreditation process may be carried out in accordance with an accreditation strategy appropriate to the particular SYSTEM and defined by the SAA.

EVALUATION AND CERTIFICATION

55. The hardware, firmware and software security features of such SYSTEM shall be evaluated and certified as being capable of safeguarding information at the intended level of classification.

56. The requirements for evaluation and certification shall be included in system planning, and clearly stated in the SSRS.

57. The evaluation and certification process shall be carried out in accordance with commonly accepted guidelines and by technically qualified and appropriately cleared personnel acting on behalf of the SAA.

58. The teams may be provided from a nominated Member State's evaluation or certification authority or its nominated representatives, for example a competent and cleared contractor.

59. The degree of evaluation and certification processes involved may be lessened (for example, only involving integration aspects) where SYSTEMS are based on existing nationally evaluated and certified computer security products.

ROUTINE CHECKING OF SECURITY FEATURES FOR CONTINUED ACCREDITATION

60. The System operational authority shall establish routine control procedures, which shall ensure that all security features of the SYSTEM are still valid.

61. The types of change that would give rise to re-accreditation, or the types of change that require the prior approval of the SAA, shall be clearly identified and stated in the SSRS. After any modification, repair or failure, which could have affected the security features of the SYSTEM, the System Operational Authority shall ensure that a check is made to ensure the correct operation of the security features.

Continued accreditation of the SYSTEM shall normally depend on the satisfactory completion of the checks.

62. All SYSTEMS where security features have been implemented shall be inspected or reviewed on a periodic basis by the SAA. In respect of SYSTEMS handling TOP SECRET or special category information the inspections shall be carried out not less than once annually.

CHAPTER VII

COMPUTER EQUIPMENT

SECURITY OF MICROCOMPUTERS/PERSONAL COMPUTERS

63. Microcomputers/Personal Computers (PCs) with fixed disks (or other non-volatile storage media), operating either in stand-alone mode or as networked configurations, and portable computing devices (for example, portable PCs and electronic "notebooks") with fixed hard disks, shall be considered as information storage media in the same sense as floppy diskettes or other removable computer storage media.

64. This equipment shall be afforded the level of protection, in terms of access, handling, storage and transportation, commensurate with the highest classification level of information ever stored or processed (until downgraded or declassified in accordance with approved procedures).

USE OF PRIVATELY-OWNED IT EQUIPMENT FOR OFFICIAL WORK

65. The use of privately-owned removable computer storage media, software and IT hardware (for example, PCs and portable computing devices) with storage capability shall be prohibited for handling classified information.

66. Privately owned hardware, software and media shall not be brought into any area where classified information is handled without the permission of the Head of the Security Office or of a Member State's Department.

USE OF THE CONTRACTOR-OWNED OR NATIONALLY-SUPPLIED IT EQUIPMENT FOR OFFICIAL WORK

67. The use of contractor-owned IT equipment and software in organisations in support of official work may be permitted by the Head of the Security Office or of a Member State's Department. The use of nationally-provided IT equipment and software may also be permitted. In this case, the IT equipment shall be brought under the control of the appropriate inventory. In either case, if the IT equipment is to be used for handling classified information, then the appropriate SAA shall be consulted in order that the elements of INFOSEC that are applicable to the use of that equipment are properly considered and implemented.

PLANNING THE LIFECYCLE

68. Hardware or software should be procured after approval by the SAA. In deciding whether equipment, particularly computer storage media, should be leased rather than purchased, it should be borne in mind that such equipment, once used for handling classified information, cannot be released outside an appropriately secure environment without first being declassified to the approval of the SAA and that such approval may not always be possible.

ANNEX A DEFINITIONS

CERTIFICATION shall mean: The issue of a formal statement, supported by an independent review of the conduct and results of an evaluation, of the extent to which a SYSTEM meets the security requirement, or a computer security product meets pre-defined security claims.

COMMUNICATION CONTROLS incorporate boundary protection devices such as firewalls, intrusion detection systems, sandboxes, honey pots etc. intended to prevent unauthorised intrusion into the IT system.

COMPUTER SECURITY PRODUCT shall mean: A generic computer security item which is intended for incorporation into an IT system for use in enhancing, or providing for, confidentiality, integrity or availability of information handled.

EVALUATION shall mean: The detailed examination, by an appropriate authority, of the security aspects, technical and non-technical, of a SYSTEM or of a cryptographic or a computer security product.

Notes: (1) The evaluation investigates the presence of required security functionality and the absence of compromising side-effects from such functionality and assesses the incorruptibility of such functionality; and

(2) The evaluation determines the extent to which the security requirements of a SYSTEM, or the security claims of a computer security product, are satisfied and establishes the assurance level of the SYSTEM or of the cryptographic, or the computer security product's trusted function.

INFORMATION SECURITY (INFOSEC) shall mean: The application of security measures to protect information processed, stored or transmitted in communication, information and other electronic systems against loss of confidentiality, integrity or availability, whether accidental or intentional, and to prevent loss of integrity and availability of the systems themselves. INFOSEC measures include those of computer, transmission, emission and cryptographic security, and the detection, documentation and countering of threats to information and to the SYSTEMS.

IT AREA shall mean: An area that contains one or more computers, their local peripheral and storage units, control units and dedicated network and communications equipment.

Note: This does not include a separate area in which remote peripheral devices or terminals/workstations are located even though those devices are connected to equipment in the IT area.

IT NETWORK shall mean: Organisation, geographically disseminated, of IT systems interconnected to exchange data, and comprising the components of the interconnected IT systems and their interface with the supporting data or communications networks.

Notes: (1) An IT network can use services of one or several communications networks interconnected to exchange data; several IT networks can use the services of a common communications network.

(2) An IT network is called “local” if it links several computers together in the same site.

IT NETWORK SECURITY FEATURES include the IT system security features of individual IT systems comprising the network together with those additional components and features associated with the network as such (for example, network communications, security identification and labelling mechanisms and procedures, access controls, programs and audit trails) needed to provide an acceptable level of protection for classified information.

IT SYSTEM shall mean: Assembly of equipment, methods and procedures, and if necessary, personnel, organised to accomplish information processing functions.

Notes: (1) This is taken to mean an assembly of facilities, configured for handling information within the system;

(2) Such systems may be in support of consultation, command, control, communications, scientific or administrative applications including word processing;

(3) The boundaries of a system will generally be determined as being the elements under the control of a single System Operational Authority; and

(4) An IT system may contain subsystems some of which are themselves IT systems.

IT SYSTEM SECURITY FEATURES comprise all hardware/firmware/software functions, characteristics, and features; operating procedures, accountability procedures, and access controls, the IT area, remote terminal/workstation area, and the management constraints, physical structure and devices, personnel and communications controls needed to provide an acceptable level of protection for classified information to be handled in an IT system.

REMOTE TERMINAL / WORKSTATION AREA shall mean: An area containing some computer equipment, its local peripheral devices or terminals/workstations and any associated communications equipment, separate from an IT area.

SPECIAL CATEGORY: Additional markings such as CRYPTO or any other special handling designator, shall apply where there is a need for limited distribution and special handling in addition to that designated by the security classification.

SSRS shall mean: SYSTEM-Specific Security Requirement Statement. It will contain as a minimum:

a) A statement of the objective of accreditation for the system; in particular, what classification level(s) of information are to be handled and what system or network security mode(s) of operation is being proposed;

b) Production of a risk management review to identify the threats and vulnerabilities and measures to counter them;

c) The Security Operating Procedures (SecOPs) with a detailed description of the proposed operations (e.g., modes, services, to be provided) and including a description of the SYSTEM security features which shall form the basis of accreditation;

d) The plan for the implementation and maintenance of the security features;

e) The plan for initial and follow-on system security or network security test, evaluation and certification; and

f) Certification, where required, together with other elements of accreditation.

TEMPEST countermeasures: security measures intended to protect equipment and communication infrastructures against the compromise of classified information through unintentional electromagnetic emissions.