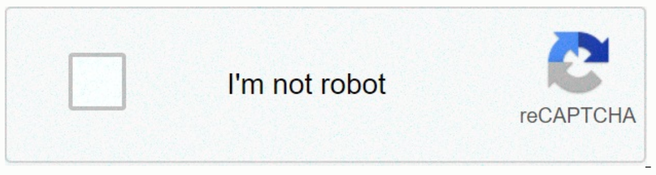


Continue

# Dod automated information system definition

in: Hardware, Definition, Data, Computing Edit Share An Automated Computer System (AIS) is [a] generic term applied to all electronic computing systems. Automated Computer Systems (AIS) collects, stores, processes, creates, broadcasts, communicates or controls data or information. AIS are composed of computer hardware (e.g. automated data processing equipment and associated devices that may include communication equipment), firmware, an operating system (OS) and other applicable software. [1] [in the assembly of hardware, software and firmware used for electronic data entry, processing, storage and/or output. Examples include: mainframes, servers, desktop workstations, thin customers, and mobile devices (e.g. laptops, electronic readers, smartphones, tablets). Typically, system components include, but are not limited to: Central Processing Units (Processors), monitors, printers, switches, routers, media converters, and removable media, would be flash drives. An AIS may also include non-traditional peripheral equipment, such as digital network copiers, and audio recording/playing devices used to transfer data to or from a computer. [3] [an] automated process in which machines perform data operations, thereby reducing the need for human intervention. [4] References[edit | source editing] Hardware Definition Data Computing Community content is available under CC-BY-SA, unless otherwise stated. An automated computer system (AIS) is a computer hardware system, computer software, data and/or telecommunications that performs functions such as the collection, processing, storage, transmission and display of information. Program managers (PM) for AIS application purchases are responsible for coordinating with organizations that will host (execute) applications at the beginning of the acquisition process. The PM must address the operational security risks that the ISA may impose on the organisation, as well as the identification of all system security needs that can be addressed more easily by organisational services than by system improvement. Basic Information Assurance (AI) controls serve as a common framework for facilitating this process. The designated approval authority for the organisation receiving an AIS application is responsible for incorporating AI considerations for the AIS application into the Enclave's Information Assurance Plan (ISP). The task of ensuring that an AIS application has adequate assurance is a shared responsibility of both the AIS PM application and the approval authority designated for the hosting organization; however, the responsibility for initiating this negotiation process is clearly the PM. based on the common capabilities of AI that can be provided by the hosting organisation. [1] A major automated computer system (MAIS) is a procurement program for an automated computer system. AcqLinks and References: [1] Defense Acquisition Guidebook (DAG) Updated: Updated: DIRECTIVE OF THE DEPARTMENT OF DEFENCE NUMBER 5200.28 21 March 1988 USD(A) SUBJECT: Security requirements for automated computer systems (AISS) References: (a) Directive DoD 5200.28, Security requirements for automatic data processing systems (ADP), 18 December 1972 (hereby cancelled) (b) DoD 5200.1-R, Information Security Program Regulation, June 1986, authorised by DoD Directive 5200.1, 7 June 1982 (c) DoD Directive C-5200.5 , Communications Security (COMSEC) (U) 6 October 1981 (d) DoD Directive S-5200.19, Controlling Compromising Emanations (U) 10 February 1968 (e) by (v), see Precinct E1. 1. REEMITION AND SCOPE OF THIS Directive: 1.1. Reissue and revise reference (a) to update the uniform policy in addition to the policy referred to in point (b) for the protection of classified, sensitive unclassified and unclassified information processed in the IAS. 1.2. Updates the dod program for automated computer system security (AIS). 1.3. Provides mandatory and minimum ISA security requirements. Stricter requirements may be required for certain systems on the basis of an assessment of acceptable risk levels. 1.4. Promotes the use of cost-effective, computer-based security features (e.g. hardware, software and firmware) for AIS. However, it is stressed that system users have a personal responsibility to protect information classified in accordance with reference paragraph 10-101.a. (b). 1.5. Requires a more precise specification of the general DoD security requirements for AIs that process classified or sensitive unclassified information. 1.6. Stresses the importance of a lifecycle management approach for the implementation of IT security requirements. 2. APPLICABILITY AND APPLICATION 2.1. This Directive shall apply to the Office of the Secretary of Defence (OSD), the military departments and military services within those departments, the Joint Chiefs of Staff (JCS), the Joint Staff, the united and specified commanders, the defence agencies, the doD's field activities and other offices, agencies, activities and orders which may be established or designated by law by the President or the Secretary of Defence (collectively referred to as DoD Components). 2.2. This Directive shall apply to the following categories of information: 2.2.1. Classified information. Thus, the completion of DoD 5200.l-R (reference (b)) for such information when contained in the ISS. 2.2.2. Sensitive information not classified. 2.2.3. Unclassified information. 2.3. This Directive shall apply to all IAS, including independent systems, communication systems and computer network systems of all sizes, digital, analogue or hybrid; peripheral devices and associated software; control computers built-in it systems; communications switching computers; personal computers; smart terminals; word processors; office automation systems; application and operating system software; firmware; and other AIS technologies, after they can be developed. Developed. This Directive, Reference (b) and DoD Directive C-5200.5 (reference (c)) shall apply to means of transport and communications connecting components of or to an ISA. 2.5. This Directive, DoD Directive S-5200.19 (reference (d)), NACSI 5004 (reference (e)) and NACI 5005 (reference (f)) apply to isa safety requirements. 2.6. This Directive and DCID No 2.6. 1/16 (reference (g)) applies to ISAs that process foreign information and/or counterintelligence. 2.7. This Directive and SM-313-83 (reference (h)) apply to IAS which processes a single highly sensitive integrated operational-information plan (SIOP-ESI). 2.8. This Directive and Instruction DoD 5215.2 (reference (i)) apply to the reporting and dissemination of ais technical vulnerabilities and corrective measures. 2.9. All IAss handling classified, sensitive, unclassified or unclassified information shall comply with the relevant requirements of this Directive. Unless the designated approval authority (DAA) requests otherwise, AIss meeting any of the following conditions are excluded from meeting policy subsections 4.5. in point 4.7, below, of this Directive: 2.9.1. AIss that are operated only in dedicated security mode. 2.9.2. Personal computers, text processors and similar stand-alone AIss in which it is not technically feasible to configure the equipment to support internal security controls. Such AIss can be characterized as single-state machines without a set of privileged instructions or memory-blocking features, and must be operated only in the dedicated mode. 2.9.3. An AIS that is embedded in a larger system and is not easily removed, is user-free and normally receives input from or outputs only to other parts of the system. 2.10. ISA networks should be examined on a case-by-case basis for the application of the policy in this Directive. The Network DAA should obtain guidance through established command channels from the National Security Agency. (NSA) or, where appropriate, from the Defence Information Agency (DIA) on evaluation and accreditation (see premises E5.). 3. DEFINITIONS The terms used in this Directive are defined in the E2 premises. 4. Policy DoD policy is the one that: 4.1. Classified and sensitive non-classified information shall be protected at all times while in the IAS. The guarantees shall be applied in such a way that this information is accessed only by authorised persons, is used only for the intended purpose, preserves the integrity of the content and is duly marked as necessary. Where classified information is involved, the information security requirements of DoD 5200.1-R (reference (b)) must be met. 4.2. Information not classified in submitted in the AIS must be protected against manipulation, loss and destruction and are available when necessary. This is necessary to protect DoD's investment in obtaining and using information and to prevent fraud, waste and abuse. The suggested guarantees for unclassified information are in OMB Circular No. A-130 A-130 (j)) and include applicable staff, physical, administrative and technical checks. 4.3. The protection of Information and resources of THE ISA (against sabotage, fraudulent manipulation, denial of service, espionage, fraud, diversion, misuse or release to unauthorised persons) is achieved by the continuous hiring of guarantees consisting of administrative, procedural, physical and/or environmental measures, personnel, security of communications, security of fumes and computer security (e.g. hardware, firmware and software), as appropriate. The mixture of selected guarantees achieves the required level of security or protection. 4.4. The mix of guarantees selected for an AIS processing classified or sensitive unclassified information shall ensure that the AIS meets the minimum requirements laid down in premises E3. These minimum requirements must be met by automatic and manual means, in a cost-effective and integrated manner. An analysis shall be carried out using the E4 enclosure. identification of any additional requirements in addition to the set of minimum requirements. 4.5. The IT security characteristics of commercially manufactured products and government-developed or derived products shall be assessed (as requested) to be designated as reliable IT products with a view to inclusion in the list of evaluated products (EPL). The products evaluated are designated as meeting the security criteria maintained by the National Computer Security Centre (NSC) at the NSA, defined by the security division, class and feature (e.g. B, B1, access control) described in DoD 5200.28-STD (reference (k)). 4.6. The following timetable shall be observed: 4.6.1. All IAS processing or managing classified and/or sensitive information not classified and requiring at least controlled access protection (e.g. Class C2 security), based on the risk assessment procedure described in premises E4, shall implement the necessary security features by 1992. 4.6.2. Where the above-mentioned safety features of Class C2 are required for an AIS, based on the risk assessment procedure described in premises E4. These requirements are met either by implementing the trusted IT products listed on the EPL or by using a product that does not apply to EPL and which has security features that meet the level of trust required for the AIS. In both cases, in order to assess whether appropriate security measures have been taken to enable the operational use of the ISA, accreditation by the DAA must be carried out and approved. 4.7. There are cases where the introduction of additional security features on the computer, in accordance with the timetable set out in subsection 4.6. In such cases, the following shall apply: 4.7.1. Other safeguards (e.g. physical controls, administrative controls, etc.) may be replaced as long as the necessary level of security or system protection is reached, as determined by the DAA. 4.7.2. Exceptions to subsection 4.6., above, may be authorised only by the head of the DoD component or by a senior DAA appointed by the head of the DoD component. This authorisation is based on a written determination that one or more of the conditions of subsection 4.7., above, exist one or more of the conditions of subsection 4.7. Exceptions shall be reviewed with each re-accreditation. 4.8. When the AIS managed by different DAAs are interface or network, a Memorandum of Understanding (MOA) is required to meet the accreditation requirements for each AIS involved. THE MOA should include the description and classification of the data; the user's licensing levels; designation of DAA to resolve conflicts between DAA; guarantees to be implemented before interspersing AI. MoAs are required when a DoD AIS component interfaces with another AIS within the same DoD component or in another DoD component and when a contractor's AIS interfaces with the AIS of one DoD component or another contractor's AIS. 4.8.1. For a multi-user telecommunications network (e.g. defence data network or global military command and control system intercomputer network), a DAA is designated as responsible for overall network security and sets out security and protection requirements for connecting The ISA to the network. 4.8.2. The necessary guarantees are agreed and implemented and the IAS are accredited for interconnection before connecting to the network. 4.8.3. The security of each AIS connected to the network remains the responsibility of the DAA. 4.8.4. The DAA responsible for the overall security of the network has the authority and responsibility to remove from the network any AIS that does not adhere to the security requirements of the network. 4.8.5. It is permissible to define network interfaces and boundaries in manageable subnets based on physical or logical limits when it is necessary to do so. Cryptographic separation and/or equivalent computer security measures as defined by the NSAs or DEA, as appropriate, constitute a basis for defining such interfaces or network and/or subnet limits. 4.8.6. Networks, including all connected subnets, shall be accredited for the highest required division and security class on the basis of the concepts and procedures in the E4 premises. and E5. 4.9. The security policy shall be taken into account throughout the life cycle of an ISA from the beginning of concept development, through design, development, operation and maintenance to replacement or disposal. DaA is designated as responsible for the overall security of the AIS. meet the following conditions: 4.9.1. The AIS developer is responsible for ensuring the early and continuous involvement of users, users, system security officers, data owners and DAA(i) in defining and implementing THE security requirements of the ISA. There must be an evaluation plan for the ISA that is progressing towards fully complying with the declared security requirements by using the necessary IT security safeguards. 4.9.2. Mandatory declarations of safeguard requirements shall be included, where appropriate, in the procurement and procurement specifications for the IAS. The declarations are the result of an initial risk assessment and specify the level of confidence required under DoD 5200.28-STD (reference (k)). 4.9.3. Classified or sensitive data not classified in an AIS shall not be entered without the designation of the classification and sensitivity of the data. The data entry approval shall be obtained from the data owner, as appropriate. 4.9.4. Accreditation of an ISA shall be supported by a certification plan, a risk analysis of the AIS in its operational environment, an assessment of security guarantees and a certification report, all approved by the DAA. Accreditation of computers embedded in a system can be system-wide. 4.9.5. A programme shall be set up to periodically verify the adequacy of guarantees for operational and accredited IAS. As far as possible, reviews shall be carried out by persons independent of the user organisation and the AIS operation or facility. 4.9.6. If necessary, as specified in OMB Circular No. A-130 (reference (j)), a programme for drawing up and testing contingency plans shall be established. The objective of contingency planning is to ensure a reasonable continuity of ISA support in the event of events that impede normal operations. Plans should be tested periodically under realistic operational conditions. 4.9.7. Changes affecting the security of an ISA should be anticipated. Any change in the AIS or associated environment that affects accredited warranties or results in changes in prescribed security requirements requires re-accreditation. Reaccreditation shall take place before the revised system is declared operational. At least, an AIS will be re-accredited every 3 years, regardless of changes. 4.10. Access by foreign nationals to an AIS owned by the U.S. government or the U.S. government may only be authorized by the DoD Component Head and must be consistent with the Department of Defense, the State Department (DoS) and the Director of Central Intelligence Policy (DCI). 4.11. An Accredited AIS for the processing and/or storage of compartmentalized sensitive information (SCI) may use automated means (software, firmware or hardware) to enable the extraction of non-SCI classified data from the SCI system for use at non-SCI classified level. This capacity is permitted only if it has been considered and approved as part of the security

accreditation, AIS operates at a minimum security class in B1. 5. RESPONSIBILITIES 5.1. Deputy Secretary of Defence (Command, (Command, Communications and information) [ASD(C3I)] must: 5.1.1. Supervise and review the implementation of this Directive. 5.1.2. Elaboration of general AIS security policies and procedures in accordance with U.S. national policies and directives in coordination with the Undersecretary of Defence (Policy) [USD(P)] and in line with DoD 5200.1-R policies (reference (b)), DoD Directive 7920.1 (reference (l)), DCID no. 1/16 (reference (g)) and Instruction DoD 5210.74 (reference (m)). 5.1.3. Promulgate instructions, standards, manuals and other broadcasts, as appropriate, in accordance with this Directive. 5.1.4. Represents the Department of Defence on the inter-agency committees involved in the development of security policy, standards and criteria for AIss. 5.2. The Deputy Undersecretary of Defence (Policy) (DUSD(P)) will continue to review, supervise and formulate general policies governing the DoD's security practices and programmes to include the development, coordination and presentation of DoD positions on the following: 5.2.1. Information security. 5.2.2. Physical security. 5.2.3. Personnel security. 5.2.4. Industrial security. 5.3. The Director of the Defence Investigation Service (DIS) shall implement an AIS security programme for the AIS of the DoD contractor in accordance with DoD Directive 5220.22 (reference (n)) and DoD 5220.22-R (reference (o)). 5.4. The Director of the Defence Communications Agency (DCA) shall implement an AIS security programme for long-distance communication systems that do not manage sci-first and certify devices performing secure or protected telecommunications switching functions. 5.5. The Director of the Defence Intelligence Agency (DIA) shall implement a program for the security of AIS and Component and DoD Component and DoD component stools and networks (e.g. the DoD Intelligence Information System) that manages the SCI. 5.6. National Security Agency and/or Central Security Service (NSA/CSS): 5.6.1. Deploy an AIS security program for all ISIs under NSA/CSS jurisdiction, including those of NSA/CSS contractors. 5.6.2. After requesting, provide doD components with communications and IT security assistance in support of effective ais security measures. 5.6.3. Establishing and maintaining technical standards and criteria for the evaluation and certification of reliable IT products. Review DoD 5200.28-STD (reference (k)) at least annually and provide recommendations for the review of ASD(C3I). 5.6.4. Providing training for DoD components in the assessment techniques and procedures applicable to sending (k) and certifying these DoD components for carrying out evaluations. 5.6.5. software products intended for use by DoD Components or contractors as trusted IT products. These assessments may be carried out on IT products developed or derived either from industrial or government sources. Also, to carry out quality assurance and to evaluations carried out by DoD Components. 5.6.6. Maintaining and publishing EPL of the evaluated industry and reliable IT products developed or derived by the government. 5.6.7. To carry out, approve and sponsor research and development of techniques and equipment for reliable IT products and for methods and techniques for assessing and verifying computer security. 5.6.8. Serve as a focal point for technical aspects related to the use of trusted IT products and systems and, with the work of testing and assessing the security of DoD Component computers, provide technical advice to DoD components on the use of trusted products and systems. 5.6.9. Ensure that assessments of AIS security posts carried out in accordance with the DoD Computer Security Programme are incorporated into the objectives and objectives of the NCCSc. 5.6.10. Assesss the overall security position of the ISS and disseminates information on hostile threats against DoD ISAs on an annual basis. 5.6.11. Operate a central technical centre to provide, after requesting, technical assistance for the assessment and certification of THE IT security elements of the AIS used in operational environments. 5.6.12. Prescribe minimum security standards, methods and procedures for the protection of classified and sensitive technical security material, techniques and information of an AIS. 5.6.13. Review and approval of standards, techniques, systems and equipment for the security of telecommunications and automated information systems. 5.7. Joint Chiefs of Staff (JCS): 5.7.1. Implementation of an AIS security programme under this Directive and SM-313-83 (reference (h)) for The AIS of DoD components and their contractors handling SIOP-ESI. 5.7.2. Providing a source of education and training for AIS security managers through the Institute of Computer Science of the Department of Defence (DoDCI) of the National Defence University (NDU) (DoD Directive 5200.2 (reference (p)). 5.8. Heads of DoD Components: 5.8.1. Implementation and maintenance of a general AIS security programme designed to ensure compliance with this Directive. 5.8.2. Ensure that contractual requirements for the protection of classified and sensitive unclassified information are provided to their contractors. 5.8.3. Ensure that funding and resources are programmed for staff, training and support for this AIS security programme and for the implementation of AISs guarantees, as appropriate, within the DoD component. 5.8.4. Designates the official(s) as the DAA (e.g. the senior AIS policy official) responsible for the accreditation of each ISA under its jurisdiction and for ensuring compliance with the AIS security requirements. 5.8.5. Establishing and maintaining an AIS Security Training and Awareness Programme all military, civilian and DoD contractor personnel requiring access to the AIss. 5.8.6. Ensure that regular independent reviews of the security and protection of the AIS are carried out to ensure compliance with the declared AIS security objectives. These reviews may be carried out using the procedures of DoD Directive 5010.38 (reference (q)). 5.8.7. Support the security of your computer Vulnerability reporting programme in accordance with Instruction DoD 5215.2 (reference (i)). 5.9. Each designated approval authority (DAA) shall: 5.9.1. Review and approval of AIS security guarantees and issuance of accreditation declarations for each AIS under DAA jurisdiction, based on the acceptability of security guarantees for ISA. 5.9.2. Ensure that all necessary safeguards, as stated in the accreditation documentation for each ISA, are implemented and maintained. 5.9.3. Identify security deficiencies and, where deficiencies are serious enough to prevent accreditation, take measures (e.g. allocate additional resources) to achieve an acceptable level of security. 5.9.4. Ensure that a Computer System Security Officer (ISSO) is appointed for each AIS and receives the training applicable to the performance of the tasks of this function. It is recommended that the ISSO not report to the operational elements of the ISA on which the security requirements of this Directive are to be implemented. 5.9.5. Request that an AIS security education and training programme be in place. 5.9.6. Make sure that ownership of the data is established for each ISA to include responsibility, access rights and special handling requirements. 5.10. Each computer system security officer (ISSO) shall: 5.10.1. Ensure that AIS is operated, used, maintained and removed in accordance with internal security policies and practices. 5.10.2. Have the authority to implement security policies and safeguards for all personnel having access to the ISA for which the ISSo is aware. 5.10.3. Ensure that users have the necessary security authorisations for personnel, authorisation and need to know, have been indoctrinated and are familiar with internal security practices prior to access to the ISA. 5.10.4. Make sure that audit tracks are reviewed periodically. 5.10.5. Start protection or correction measures if there is a security issue. 5.10.6. Report security incidents in accordance with DoD 5200.1-R (reference (b)) and DAA when an AIS is involved. 5.10.7. Report the security status of the AIS as required by the DAA. 5.10.8. Assess known vulnerabilities to determine whether additional safeguards are required. 5.10.9. Maintain a plan to improve system security and progress towards achieving accreditation. 6. DATE OF INTRODUCTION INTO FORCE AND IMPLEMENTATION 6.1. This Directive shall enter into force immediately. 6.2. Accreditations made using the requirements of the earlier version of this Directive shall remain valid but shall be updated within three years of the date of this Directive. 6.3. IAS that have started the design phase of the life cycle process the date of this Directive shall be accredited within three years of that date or before the initial operational capacity. 6.4. Each Head of Component of the DoD shall submit an implementation plan for compliance with this Directive to the Deputy Secretary of Defence for Command, Control, Communications and Information (ASD(C3I)) within 180 days of the date of this Directive This Directive shall be implemented without new Issues of DoD Components. Enclosures - 5 1. References, continuation 2. Definitions 3. Minimum security requirements 4. Procedure for determining minimum computer security requirements AIS 5. E1 network considerations. INCINT 1 REFERENCE, continuation (e) National Communications Security Instructions 5004, Tempest Measurements for Facilities Within the United States, 1 January 1984 (f) National Communication Security Instruction 5005, TEMPEST Securities for Facilities Outside the United States, 1 January 1984 (g) Director of Central Intelligence Directive No. Security Policy on Information Information in Automated Systems and Networks (U), 4 January 1983 (h) SM-313-83, Protection of the Single Integrated Operational Plan (U) 10 May 1983 (i) DoD Instruction 5215.2, Computer Security Technical Vulnerability Reporting Program, 2 September 1986 (j) Management Office and Budget Circular No. A-130, Federal Information Resource Management, December 12, 1985 (k) DoD 5200.28-STD, Department of Defense Reliable Computer System Assessment Criteria, December 1985, authorised by Directive DoD 5200.28, 18 December 1972 (l) Directive DoD 7920.1, Life-Cycle Management of Automated Information Systems (AIS), 17 October 1978 (m) DoD Instruction 5210.74, Security of DoD Contractor Telecommunications, 26 June 1985 (n) DoD Directive 5220.22 , Industrial Security Program, 1 November 1, 1986 (o) DoD Regulation 5220.22-R, Industrial Security Regulation, December 1985, authorised by DoD Directive 5220.22, 8 December 1980 (p) DoD Directive 5200.2, DoD Personnel Security Programme, 8 December 1980 (p) DoD Directive 5200.2, DoD Personnel Security Programme 5220.22 December, 8 December 1980 (p) DoD Directive 5200.2, DoD Personnel Security Programme , 8 December 1980 (p) DoD Directive 5200.2, DoD Personnel Security Programme, 8 December 1980 (p) DoD Directive 5200.22 20, 1979 (q) Directive DoD 5010.38, Internal Management Control Programme, 16 July 1984 (r) Executive Order 12356, National Security Information, 6 April 1982 (s) DoD Directive 5230.24 , Distribution Statement on Technical Documents, 18 March 1987 (t) DoD 5200.28-M , ADP Security Manual, January 1973, authorised by DoD Directive 5200.28, 18 December 1972 (u) CSC-STD-003-85, Computer Security Requirements, 25 June 1985 (v) NSC-TG-005, Version 1, Reliable Network Interpretations, 31 July 1987 E2. INCINT 2 DEFINITIONS E2.1.1. Access. A specific type of interaction between a subject (for example, person, process, or input device) and an object (for example, an AIS resource, such as a record, a file, a program, an output device) that leads to the flow of information from one to another. Also, the ability and ability to obtain knowledge of classified, sensitive information or unclassified. E2.1.2. Responsibility. Property that allows activities on an AIS to be tracked to people who can then be held responsible for their actions. E2.1.3. Accreditation. An official declaration by the DAA that the AIS is authorised to operate in a certain security manner using a set of prescribed safeguards. Accreditation is the official management authorisation for the operation of an ISA and based on the certification process, as well as other management considerations. The accreditation declaration applies the security responsibility with the DAA and shows that due attention has been taken to security. E2.1.4. AIS security. Measures and controls that protect or protect an ISA against unauthorised (accidental or intentional) disclosure, alteration or destruction of AIS and data, as well as against refusal of notification or communication. AIS security includes consideration of all functions, features and/or hardware and/or software features; operational procedures, accountability procedures and access controls to the central computer installation, remote computer and terminal installations; management constraints; physical structures and devices; and the personnel and communication controls necessary to ensure an acceptable level of risk for the ISA and for the data and information contained in the ISA. This includes all the security safeguards required to ensure an acceptable level of protection for an ISA and for data managed by an ISA. E2.1.5. Insurance. A reliable measure that the security features and architecture of an AIS accurately mediate and apply security policy. Where the security features of an ISA are invoked to protect classified or sensitive unclassified information and to restrict user access, the characteristics must be tested to ensure that the security policy is implemented and cannot be circumvented during the operation of the AIS. E2.1.6. Audit. An independent review and review of the system's records and activities to test the adequacy of system controls, to ensure compliance with established operational policy and procedures and to recommend any indicated changes to the controls, policy or procedures. E2.1.7. Audit trail. A chronological record of the system's activities that is sufficient to allow the reconstruction, review and examination of the sequence of environments and activities that surround or lead to an operation, procedure or event in a transaction from its inception to the final results. E2.1.8. Automated Computer Systems (AIS). A set of computer hardware, software, and/or firmware configured to collect, create, communicate, calculate, disseminate, process, store, and/or control data or information. E2.1.9. Category. A group of classified or sensitive non-classified information to which an additional restrictive label applies to indicate that staff are granted access to the information only if they have official access approval or other applicable authorisation (e.g. proprietary information, for official use only, compartmentalized information). E2.1.10. Certification. technical requirements of the aiss security elements and other safeguards, carried out in support of the accreditation process, which determines the extent to which a particular design and implementation of the ISA meets a specified set of security requirements. E2.1.11. Classified information. Information or materials that are (a) owned, produced for or by or under the control of the United States of America and (b) established in accordance with E.O. 12356 (reference (r)) or previous orders, DoD 5200.1-R (reference (b)), in order to seek protection against unauthorised disclosure; and thus designated. E2.1.12. Computer. A machine capable of accepting, calculating or manipulating or storing data. It usually consists of an arithmetic and logical unit and a control unit and can have input and output devices and storage devices. E2.1.13. Data. A representation of facts, concepts, information or instructions appropriate for communication, interpretation or processing by humans or by an ISA. E2.1.14. Data integrity. The state that exists when the data is unchanged from the source and accidentally or maliciously has not been altered, altered, or destroyed. E2.1.15. Data owner. The authority, person or organisation which has initial responsibility for the data by statute, executive order or directive. E2.1.16. Dedicated security mode. An operating mode in which all users have authorization or authorization and must know all data managed by AIS. If AIS processes special access information, all users require formal access approval. In dedicated mode, an ISA can manage a single classification level and/or an information category or a series of classification levels and/or categories. E2.1.17. Refusal of service. Actions or actions resulting in the inability of an ISA or any essential party to carry out its designated mission, either through loss or degradation of operational capacity. E2.1.18. Designated Approval Authority (DAA). The official who has the authority to decide on the acceptance of the security guarantees provided for an AIS or the official who may be responsible for issuing an accreditation declaration recording the decision to accept those guarantees. The DAA shall be at organisational level, have the authority to assess the general requirements of the AIS mission and provide definitive directions to AIS developers or owners regarding the risk in the Security Position of the ISA. E2.1.19. Built-in system. An embedded system is one that performs or controls a function, in whole or in part, as an integral element of a larger system or subsystem (e.g. ground support equipment, flight simulators, engine test stands or fire control systems). E2.1.20. List of products evaluated (EPL). A documented inventory of equipment, hardware, software and/or firmware that were evaluated according to the evaluation criteria found in DoD 5200.28-STD (reference (k)). E2.1.21. Features. (See Security Features, definition E2.1.40., below.) E2.1.22. Formal approval of access. Approval documented by a data owner to allow access to a category of information. E2.1.23. Handled by. The term managed by denotes the activities carried out on data in an ISA, would be collection, processing, transfer, storage, retrieval, sorting, transmission, dissemination and control. E2.1.24. Information. Knowledge such as facts, data or opinions, opinions, numerical, graphic or narrative forms, oral or maintained in any environment. E2.1.25. Computer system. The collection, processing, transmission and organised dissemination of information in accordance with defined procedures, automatic or manual. E2.1.26. Responsible for computer system security (ISSO). The person responsible for the DAA for security assurance shall be provided and implemented throughout the life cycle of an AIS from the beginning of the concept development phase by designing, developing, operating, maintaining and safely removing it. E2.1.27. Smart terminal. A terminal that is programmable, capable of supporting peripheral devices, able to connect with other terminals or computers, capable of accepting additional memory, or that can be modified to have these features. E2.1.28. Multi-level security mode. An operating mode that allows two or more levels of information classification to be processed simultaneously within the same system when not all users have an authorization or formal access approval for all data managed by THE ISA. E2.1.29. Need to know. A determination made in the interest of Us national security by the custodian of classified or sensitive unclassified information, which a potential recipient is required to have access to, knowing or holding information in order to perform official tasks or services. E2.1.30. Network. A network shall consist of a communications medium and all components attached to that medium whose responsibility is the transfer of information. These components may include AIss, package switches, telecommunications controllers, key distribution centers and technical control devices. E2.1.31. Terminology of the orange book. The reference (k), also called the Orange Book, ranks AISs into four major hierarchical security divisions. Within divisions C and B there are other subdivisions called classes. These classes are also ordered in a hierarchical manner characterized by the set of computer security features they possess (see Security Features, definition E2.1.40., below). E2.1.32. Partitioned security mode. A mode of operation in which all staff have the authorisation, but not necessarily the formal approval of access and the need to know, for all information managed by the ISA. This security mode includes the compartmentalized mode defined in DCID No. 1/16, reference (g). E2.1.33. Processing of periods. A mode of operation of an AIS in which the operating security mode and/or the maximum classification of data managed by The AIS is set for a time interval (or period) and then modified for the next time interval. A period extends from any secure initialization of the AIS to the completion of any data purjari managed by the ISA during the period. E2.1.34. Purge. Removal of sensitive data from an ISA at the end of a processing period, including from AIS storage devices and other peripheral devices with storage capacity, so that is proportionate to the sensitivity of the data that the data cannot be reconstructed. An AIS must be disconnected from any external network before a purge. E2.1.35. Risk. A combination of the likelihood of a threat occurring, the likelihood that the occurrence of a threat will have a negative impact and the severity of the resulting negative impact. E2.1.36. Risk analysis. An analysis of the assets and vulnerabilities of the system to establish an expected loss of certain events based on the estimated probabilities of occurrence. E2.1.37. Risk index. The difference between the minimum authorisation or authorisation of AIS users and the maximum sensitivity (e.g. classification and categories) of data managed by AIS. E2.1.38. Risk management. The total process of identifying, measuring and minimizing uncertain events affecting ISA resources. This includes risk analysis, cost analysis, safeguard selection, security testing and assessment, implementation of safeguard measures and system review. E2.1.39. Guarantees. (See security guarantees, definition E2.1.42., below.) E2.1.40. Security features. Functions, mechanisms and security-relevant features of AIS hardware and software (e.g. identification, authentication, audit trail, access control). E2.1.41. Security mode. An operating mode in which DAA accredits an AIS to work. Inherent with each of the four security modes (dedicated, high system, multilevel, and partitioned) are restrictions on user authorization levels, formal access requirements, the need to know the requirements, and the range of sensitive information allowed on the AIS. E2.1.42. Security guarantees. Protective measures and controls that are prescribed to meet the specified security requirements for an ISA. These warranties may include, but are not necessarily limited to, hardware and software security features; operating procedures; accountability procedures; access and distribution controls; management constraints; personnel security; and physical structures, areas and devices. E2.1.43. Sensitive compartmentalized information (SCI). Classified information about or derived from sources of information, methods or analytical processes to be managed exclusively within the formal access control systems established by the Director, Central Intelligence. E2.1.44. Sensitive information not classified. Any information to which the loss, misuse or unauthorized access or modification or modification could adversely affect the US national interest, the deployment of DoD programs or the confidentiality of DoD personnel (e.g. information and information exempt from FOIA whose distribution is limited by DoD Directive 5230.24 (reference (e)).) E2.1.45. SIOP-ESI. An acronym for Single Operational Plan-Extremely Sensitive Information, a DoD Special Access Program. E2.1.46. Special access program. Any program that requires access or need controls other than those normally required for access to confidential, secret or top secret information. Secret. a programme shall include, but is not limited to, the special authorisation of the investigative requirements, the special designation of officials authorised to determine the need to know or special lists of persons determined to need to know. E2.1.47. High security system mode. A mode of operation in which all users who have access to the ISA possess a security authorisation or authorisation, but not necessarily a need to know, for all data managed by the AIS. If AIS processes special access information, all users must have formal access approval. E2.1.48. Telecommunications. Pursuant to this Directive, a general term expressing the transmission of data between computer systems and remotely located devices through an establishment which converts the necessary format and controls the transmission rate. E2.1.49. Trusted products. Products evaluated and approved for inclusion in the list of products evaluated (EPL). E2.1.50. Unclassified information. Any information which must not be protected against disclosure but must be protected against manipulation, destruction or loss caused by record value, usefulness, replacement cost or susceptibility to fraud, waste or abuse. E2.1.51. Users. Persons or processes accessing an AIS either through direct connections (e.g. through terminals) or through indirect connections (e.g. prepare input data or receive results that are not reviewed for content or classification by a responsible person). E3. INCINT 3 MINIMUM SECURITY REQUIREMENTS E3.1.1. MINIMUM SECURITY REQUIREMENTS. The following minimum requirements must be met by automatic or manual means in a cost-effective and integrated manner: E3.1.1 1. Responsibility. Safeguards must be put in place to ensure that every person with access to an ISA can be held accountable for his or her actions in the field of IsA. There must be an audit trail that provides a documented history of the use of DAIS. The audit trail shall be sufficiently detailed to reconstruct events in determining the cause or extent of the compromise in the event of a security breach or failure. To meet this requirement, the manual and/or automated audit trail shall document the following: E3.1.1.1.1. The identity of each person and device that has access to the AIS. E3.1.1.1.2. Time of access. E3.1.1.1.3. User activity is sufficient to ensure that users' actions are controlled and controlled. E3.1.1.1.4. Activities that could alter, circumvent or cancel the guarantees controlled by the ISA. E3.1.1.1.5. Security-relevant actions associated with processing periods or changing security levels or categories of information. DaA determines a review of associated audit tracks they are aware of an appropriate retention period for audit information. The decision to request an audit trail of user access to an independent, single-user AIS (e.g. personal computer (PC), memory typewriter, typewriter) should be left to the DAA's discretion. E3.1.1.2. Access. 3. 3. control policy for each ISA. It includes features and/or procedures for implementing the INFORMATION Access Control Policy within the ISA. The identification of each authorised user access to the ISA shall be established positively before access is authorised. E3.1.1.3. Security training and awareness. There must be a security training and awareness programme, with training for the security needs of all persons accessing the ISA. The Programme shall ensure that all persons responsible for the ISA and/or information within it, as well as all persons accessing the AIS, are aware of the appropriate operational and security procedures and risks. E3.1.1.4. Physical checks. The AIS hardware, software and documentation, as well as all classified and sensitive unclassified data managed by the AIS, are protected to prevent unauthorized disclosure, destruction or modification (intentional or unintentional) (e.g. data integrity). The level of control and protection shall be proportionate to the maximum sensitivity of the information and shall provide the most restrictive control measures required by the data to be handled. This includes personnel control, physical, administrative and configuration checks. In addition, protection against denial of service notification of AIS resources (e.g. hardware, software, firmware and information) must be consistent with the sensitivity of the information managed by AIS. Unclassified hardware, software or documentation of an AIS shall be protected if access to such hardware, software or documentation reveals classified information or if access provides information that may be used to remove, circumvent or otherwise render ineffective security safeguards for classified information. Software development and related activities (e.g. system analysis) are controlled by physical controls (e.g. two-person control) and protected when it is established that the software is used for handling classified or sensitive unclassified data. E3.1.1.5. Marking. Classified and sensitive unclassified production must be marked to accurately reflect the sensitivity of the information. The requirements for the security classification and the applicable markings for classified information are set out in DoD 5200.1-R (reference (b)). The marking can be automated (for example, AIS has a feature that produces the markings) or it can be done manually. Automatic exit markings shall not be considered correct unless the security features and AIS assurances meet the requirements for a minimum security class B1, as specified in DoD 5200.28-STD (reference (k)). If B1 is not met but automatic controls are used, outputs must be protected at the highest level of classification of information managed by the ISA until manual review by an authorised person to ensure that the production has been precisely marked with classification and reserves. All supports (and containers) are marked and protected in proportion to the for the highest level of security classification and the most restrictive category of information ever stored until the media are declassified (e.g. degassed or deleted) using a DoD-approved methodology set out in the DoD AIS Security Manual, DoD 5200.28-M (reference (t)) or unless the information is declassified or declassified according to reference (b). E3.1.1.6. Smallest privilege. The AIS works in such a way that each user has access to all the information to which the user is entitled (by virtue of authorization, official approval of access), but no more. In case of need to know classified information, access must be essential for the fulfilment of the legal and authorized purposes of the Government. E3.1.1.7. Continuity of data. Each file or data collection in the AIS must have an identifiable source throughout its lifecycle. Its accessibility, maintenance, movement and disposition shall be governed by security authorisation, official access approval and the need to know. E3.1.1.8. Data integrity. There must be safeguards for detecting and minimising accidental data modification or destruction and for detecting and preventing the malicious destruction or alteration of data. E3.1.1.9. Contingency planning. Emergency plans shall be drawn up and tested in accordance with OMB Circular No. A-130 (reference (j)) to ensure that AIS security controls work reliably and otherwise that adequate backup functions exist to ensure that security functions are maintained continuously during interrupted service. If the data are altered or destroyed, recovery procedures must be in place. E3.1.1.10. Accreditation. Each ISA is accredited to operate under a set of security guarantees approved by the DAA. E3.1.1.11. Risk management. There should be a risk management program to determine how much protection is needed, how much there is, and the most economical way to provide the necessary protection. E4. PROCEDURE OF INCINT 4 FOR THE DETERMINATION OF MINIMUM INFORMATION SECURITY REQUIREMENTS ON THE BASIS OF AIS E4.1.1. PROCEDURE FOR EVALUATION OF RISKS. The following risk assessment procedure is extracted from CCS-STD-003-85 (reference (u)). The procedure is used to determine the minimum assessment class required for an ISA, based on the sensitivity of the information present in the AIS and the authorisations of its users. Any DoD component wishing to use a different method to fulfil the intention of this enclosure may do so if prior approval has been granted by ASD(C3I). NOTE: In the case of a network, the procedure applies individually to each of the IAS on the network. Rating class should be considered a minimum partial requirement, as connecting an ISA to another ISA or to a network may lead to additional risks (see enclosure E5.). The DAA for a network may also decide to apply the procedure once to the network and determine the assessment class by applying the requirements of DoD 5200.28-STD (reference (k)) to the network as a whole. Whole. Step 1. Determine how system security works. The operation of the security system for an AIS is determined as follows: E4.1.1.1.1. An ISA is defined as operating in dedicated security mode if all users have authorization or authorization, documented official access approval, if necessary, and the need to know all information managed by AIS. The ISA may manage a single classification level and/or a category of information or a series of classification levels and/or categories. The AIS shall be electrically, logically and physically isolated from all personnel and DEA who do not have the necessary authorisation or authorisation, from official access approval, if necessary, and shall be aware of all information managed by the AIS. E4.1.1.1.2. An AIS is defined as operating in the system's high-security mode if all users have documented official access authorisation or authorisation and approval, if necessary, but not necessarily the need to know all the information managed by the AIS. E4.1.1.1.3. An AIS is defined as operating in multi-level security mode if not all users have approval for authorisation, authorization or official access, if necessary, for all information managed by AIS. E4.1.1.1.4. An AIS is defined as operating in partitioned security mode if all users have the authorisation, but not necessarily a formal access approval, for all information managed by the AIS. E4.1.1.2. Step 2. Determine the user's minimum clearance or authorization assessment. The minimum user clearance or authorisation (Rmin) is defined as the maximum clearance or authorisation of the least authorised or least authorised user. Rmin is determined from table E4. T1. The authorisations used in the following table are defined in DoD Directive 5200.2 (reference (p)). TABLE E4. T1. USER MINIMUM CLEARANCE OR AUTHORIZATION SCALE Blurred or unauthorized assessment (U) 0 Not removed but authorized access to non-classified sensitive information (N) 1 Confidential (C) 2 Secret (S) 3 Top Secret (TS) and/or Current Background Investigations (BI) 4 Top Secret (TS) and/or Current Special Background Investigations (BI) 5 A Category (1C) 6 Multiple Categories (MC) 7 E4.1.1.3. Step 3. Determination of the maximum assessment of data sensitivity. The maximum data sensitivity (Rmax) is determined from the following table: TABLE E4. T2. MAXIMUM DATA SENSIBILITY SCALE Maximum Sensitivity Ratings 2 No Categories Assessment Maximum Data Sensitivity With Categories 1 Evaluation (Rmax) (Rmax) (Rmax) Unclassified (U) 0 Not applicable 3 Unclassified but Sensitive 4 1 N With one or more categories 2 Confidential (C) 2 C With one or more categories 3 Secret (S) 3 S With one or more categories with no more than one secret data 4 5 Top Secret (TS) 5 5 TS with one or more categories with no more than one category containing secret data or top secret TS with two or more categories containing secret data or top secret 6 7 _____ 1 The only categories of are those for which some users are not authorized to access. When you count the number of categories, count all categories, regardless of the sensitivity level associated with the data. If a category is associated with more than one sensitivity level, it is counted only at the highest level. Systems in which all data are in the same category are treated as being without categories. 2 If the number of categories is large or where a very sensitive category is involved, a higher rating could be justified. 3 Data not classified by definition may not contain categories. 4 Examples of N data include financial, proprietary, privacy and mission-sensitive data. In some situations (e.g. those involving extremely high financial amounts or critical mission-sensitive data), a higher rating may be justified. Table E4. T2. prescribe minimal assessments. 5 The increase in rating between Secret and Top Secret data sensitivity levels is greater than the increment between other adjacent levels. This difference derives from the fact that the loss of Top Secret data causes particularly serious damage to U.S. national security, while the loss of secret data causes GRAVE damage. E4.1.1.4. Step 4. Determine the risk index. The risk index depends on the rating associated with the minimum clearance of the AIS user (Rmin) and the rating associated with the maximum classification of information managed by the AIS (Rmax). The risk index is calculated as follows: E4.1.1.4.1. Case a. If Rmin is lower than Rmax, then the risk index is determined by subtracting Rmin from Rmax. Risk Index = Rmax - Rmin NOTE: There is an abnormal resulting value because there are two types of Top Secret clearance and only one type of Top Secret data. When the user's minimum clearance is TS/BI and the maximum data sensitivity is Top Secret without categories, then the risk index is 0 (rather than the value 1, which should result from a direct application of the formula). E4.1.1.4.2. Case b. If Rmin is greater than or equal to Rmax, then: Risk index = 1, if there are categories to which some users are not authorized access, or: Risk index = 0 in all other cases. E4.1.1.5. Step 5. Determine the minimum security rating class for controls on your computer. E4.1.1.5.1. The following table is used to determine the minimum security class required for an ISA based on the risk index calculated in step 4 above. The levels in the table are those described in DoD 5200.28-STD (reference (k)). TABLE E4. T3. INFORMATION SECURITY REQUIREMENTS SSCAL Risk Index Minimum Security Mode Security Class 4 0 Dedicated 5 No Minimum Class 1.2 0 High System C2 2 1 Multilevel, B1 3 Partitioned 2 Multilevel, B2 Partitioned 3 Multilevel B3 4 Multilevel A1 5 Multilevel * 6 Multilevel * 7 Multilevel _____1 Although there is no prescribed minimum class, the integrity and service denial requirements of many systems justify at least Class C1 protection. 2 Automatic exit markings must be invoked to be accurate only class B1 is used. (See requirements for marking in premises E3.) 3 Where an ISA manages classified or compartmentalized data and some users do not have at least one confidential authorisation or where there are more than two types of managed compartmentalized information, at least one class B2 is required. 4 The asterisk (*) indicates that computer protection for environments with this risk index is considered to be beyond the state of current computer security technology. 5 Most built-in systems and desktop computers work in dedicated mode. E4.1.1.6. Step 6. Adjustments to the calculated security assessment class are required. Additional requirements or recommendations relevant to the determination of the minimum assessment class include the following: E4.1.1.6.1. If an AIS is connected to a network or other AIS, it should ensure that the AIS accreditation requirements are not breached due to the presence of network technology. E4.1.1.6.2. In the dedicated way in which AIS is connected to one or another AIS, it is recommended (although not necessary) to use at least the CI level. This recommendation is made because level C1 can provide a sufficient security measure to prevent users from accidentally modifying or deleted each other's data. E4.1.1.6.3. An AIS using processing periods (e.g. operating in one or more security modes and/or at one or more security levels for certain periods of time during which acceptable sanitisation procedures are implemented between processing periods) may have more than one risk index. In such cases, the highest value of the risk index shall be used to determine the minimum level of the safety feature. E5. INCINT 5 CONSIDERATIONS RELATING TO THE E5.1.1 NETWORK. For accreditation purposes, a network is treated either as an interconnection of accredited IAS (which can be networks) or as a unified network. These two cases are discussed below: E5.1.1.1. Case I. Accredited AISS interconnections E5.1.1.1.1. Where a network consists of previously accredited ISAs, a MEMORANDUM is required between the DAA for each AIS DoD component and the DAA responsible for the network (as provided for in Section 4 of this Directive). The DAA network shall ensure that interface restrictions and limitations are respected for connections between DoD component AIs. NCSC-TG-005 (reference (v)) provides for interface restrictions and limitations that may be applicable. In particular, the connections between the accredited IAS shall be consistent with the mode of operation of each AIS, the specific level of sensitivity or the range of sensitivity levels for which each AIS is accredited, with any additional interface constraints associated with the interface device used for connection and any other imposed by the MOA. E5.1.1.1.2. Each AIS is assigned an accreditation range, consisting of the set of security levels that can be associated with the data it sends over the network connection. If the accreditation range is greater than at a single level, the AIS must reliably separate the data by level within its accreditation range and accurately label it for multi-level interface transmission. E5.1.1.1.3. AIS dod component DAAs should be aware that connecting to a network may involve additional risks due to the potential exposure of data from your own AIS to the larger community of all AISs users on the network. As regards the connections to adjacent IAS, the operational modes and security mechanisms of these AIs should be taken into account, beyond the mere fact of their accreditation. E5.1.1.1.4. Unreliable, unaccredited AISs, either individual it systems or subnets, may also be components of a network. Connections between them and other component information systems are permitted under the same conditions as in E5.1.1.1.1. Only unclassified information, which does not include non-classified sensitive information, may be sent to and from untrusted and unaccredited IAs. E5.1.1.1.5. Special AISs or support, such as package switching nodes and terminal access interfaces, must also have received individual accreditation if they carry classified or sensitive unclassified information. The DAA network serves as dAA for all these AIss. E5.1.1.2. Case II. Unified networks E5.1.1.2.1. Some networks may be accredited as a whole without prior accreditation of each of their components. It is necessary to treat a network as unified when some of its components are so specialised or dependent on other components of the network for security assistance that individual accreditation of such components is not possible or significant with regard to the secure operation of the network. In order to be accredited, a unified network must have a coherent network security architecture and design and should be developed with attention to security requirements, mechanisms and assurances commensurate with the range of sensitivities of the information for which it is to be accredited. E5.1.1.2.2. The recommended approach to the accreditation of a unified network is the application of the E4 enclosure. network to obtain an assessment class. The requirements for the fulfilment of that assessment class are then obtained from an applicable interpretation of DoD 5200.28-STD (reference (k)), would be NCCC-TG-005 (reference (v)). (v)).