Director of Central Intelligence Directive 1/16 [1]

Security Policy for Uniform Protection of Intelligence Processed in Automated Information Systems and Networks (U)

(Effective 19 July 1988)

[1] This directive supersedes DCID 1/16 effective 4 January 1983. (U)

Pursuant to the statutory authority and responsibilities assigned to the Director of Central Intelligence for the protection of intelligence sources and methods in Section 102 of the National Security Act of 1947, Executive Orders 12333 and 12356, and National Security Decision Directive 145, policies and procedures are herewith established for the security of classified intelligence processed, communicated, or stored in automated information systems (AISs) and networks. (U)

This directive applies to all U.S. Government organizations, their commercial contractors, and Allied governments that utilize AISs and networks to process, store, and transmit U.S. foreign intelligence and counterintelligence information (hereafter referred to as intelligence) that has been classified pursuant to Executive Order 12356 (or successor order). [2] (U)

[2] "Foreign intelligence" and "counterintelligence" have the meanings assigned to them in Executive Order 12333 (or

successor order). "Intelligence" includes sensitive compartmented information, special access programs for intelligence, and other intelligence that involves sensitive sources or methods (sometimes referred to as collateral intelligence) that is or should be marked WNINTEL: intelligence that identifies or would reasonably permit identification of a source or method susceptible to countermeasures that could nullify or reduce its effectiveness. (U)

1. General Policy Guidance (U)

a. ***Policy Objectives.*** The purpose of this directive is to establish long-term (year 2000) goals and near-term (year 1992) requirements intended to improve the security of U.S. intelligence processed in AISs, and networks with respect to its possible compromise (1) due to penetration by hostile intelligence services, (2) by otherwise legitimate users who gain access to data or processes for which they are not authorized, or (3) as a result of inadequate security design, implementation, or operation. The directive also assigns policy execution roles and responsibilities, and establishes a procedural framework within which they are to be implemented. Specific guidance is provided in the Security Manual for Uniform Protection of Intelligence Processed in Automated Information Systems and Networks (Security Manual), a supplement to this directive. Additional security measures may be established by the accrediting authority if deemed appropriate. Such measures should also be in accordance with other DCIDs listed in references 9 to 13 in Annex A of the Security Manual. The provisions contained in the Security Manual have the same force as this directive. (U)

b. Trusted Systems. The criteria for characterizing the technical level of trust (i.e., standards of technical security protection) to be met by AISs processing intelligence are those set forth in Department of Defense publication 5200.28-STD, December 1985, Department of Defense Trusted

Computer System Evaluation Criteria.[3] These criteria for trusted systems establish levels of trust that represent a relative measure of an AIS's ability to protect sensitive information. A level of trust is not based solely on the presence of protection mechanisms in an AIS. Rather, it is based on the use of systems engineering discipline to properly structure the AIS and implementation analysis to ensure the AIS provides the appropriate level of trust. Therefore, a trusted system with an appropriate level of trust may be implemented by (1) using and correctly implementing products available on the National Computer Security Center's Evaluated Products List (EPL), (2) designing and implementing a new AIS to meet the specified level of trust, or (3) a combination of both. In any event, the resulting system should be evaluated in its operational environment to ensure that all appropriate criteria are satisfied. When suitable products are available on the EPL, they shall be incorporated into new systems and into the upgrade of existing systems as soon as feasible. The goal is for all Intelligence Community AISs to become trusted systems incorporating trusted products by the year 2000. (U)

[3]Modifications to this standard by DoD shall be reviewed by the DCI prior to inclusion in this directive. (U)

c. **[2 lines deleted]**

(1) **[4 lines deleted]**

(2) **[approx. 7 lines deleted]**

(3) **[approx. 2 lines deleted]**

d. **[approx. 10 lines deleted]**

2. Modes of System Operation (U)

[approx. 20 lines deleted]

The mode of operation of a network is determined by the extent to which it must reliably separate intelligence transmitted through it by AISs or other attached networks. This is determined by the classification(s) and type(s) of intelligence the network must keep separate during transmission. (U)

3. Accreditation Authority and Responsibility (U)

a. ***Definition.*** Accreditation is the official management authorization to operate an AIS or network: (1) in a particular security mode; (2) with a prescribed set of administrative, environmental, and technical security safeguards; (3) against a defined threat and with stated vulnerabilities and countermeasures; (4) in a given operational environment; (5) under a stated operational concept; (6) with stated interconnections to other AISs or networks; and (7) at an acceptable level of risk for which the accrediting authority has formally assumed responsibility. The accrediting authority formally accepts security responsibility for the operation of an AIS or network and officially declares that a specified AIS or network will adequately protect intelligence against compromise, destruction, or unauthorized alteration through the continuous employment of safeguards including administrative, procedural, physical, personnel, communications security, emanations security, and computer-based (e.g., hardware, firmware, software) controls. The accreditation statement affixes security responsibility with the accrediting authority and shows that due care has been taken for security in accordance with references 9-13 in Annex A of the Security Manual. (U)

b. **[approx. 10 lines deleted]**

[4]NFIB members with principal accrediting authority under this directive are: The DCI, DDCI, DIRNSA,

D/DIA, D/INR/DoS, AD/FBI (Intell Div), DASI/DoE, SAS/Treasury. The DCI is also the head of CIA. (U)

c. NFIB members shall establish and maintain within their agencies formal automated information system and network security programs, and require similar programs to be operated by agencies and components to which accrediting authority is delegated. The Director, Defense Intelligence Agency, shall be responsible for accreditation of the DODIIS/SCINET/DSNET-3. The Director, National Security Agency, shall be responsible for accreditation of the Community On-Line Intelligence System (COINS). (U)

d. Where an AIS or network substantially involves more than one principal accrediting authority, one shall be designated the accrediting authority by mutual agreement or, if necessary, by the Director of Central Intelligence. An AIS or network processing intelligence operated by an organization that is not part of the National Foreign Intelligence Program shall be jointly accredited by its sponsor and the most appropriate principal accrediting authority (or an appropriately authorized designee). For example, the Worldwide Military Command and Control System (WWMCCS) AISs require joint accreditation if they process intelligence contained within the scope of this directive (i.e., intelligence that identifies or would reasonably permit identification of a source or method susceptible to countermeasures that could nullify or reduce its effectiveness). (U)

e. Principal accrediting authorities shall provide for the maintenance of complete records concerning the accreditation status of AISs and networks within their purview and issue reports and notifications as specified in Chapter VIII of the Security Manual. (U)

f. **[approx. 6 lines deleted]**

[5]The DCI may authorize further delegation of accreditation authority for multilevel and compartmented mode systems in specific cases upon application. (U)

[6] ibid.

g. The Intelligence Community Staff shall act for the Director of Central Intelligence in matters pertaining to the administration of this directive. (U)

4. Exclusions (U)

a. U.S. national telecommunications systems (e.g., AUTODIN, DDN, DTS), including technical control centers related thereto, which are accredited in accordance with national telecommunications policies, are not within the scope of this directive. (U)

b. **[approx. 7 lines deleted]**

c. Nothing in these provisions or in the Security Manual supersedes requirements under the Atomic Energy Act of 1954, as amended (Section II, Public Law 585), on the control, use, and dissemination of Restricted Data or Formerly Restricted Data, or requirements regarding Communications Security (COMSEC)-related material as established by or under existing statutes or successors, directives, or Presidential policy. (U)

Supplement:
Security Manual for Uniform Protection
of Intelligence Processed in Automated
Information Systems and Networks
