DIRECTOR OF CENTRAL INTELLIGENCE DIRECTIVE 6/3
PROTECTING SENSITIVE COMPARTMENTED INFORMATION WITHIN INFORMATION SYSTEMS

POLICY

(Effective 05 June 1999)

This directive is promulgated pursuant to authorities andresponsibilities assigned to the Director of Central Intelligence (DCI) for the protectionof intelligence sources and methods. These DCI authorities and responsibilities may befound in the National Security Act of 1947, as amended; in Executive Orders 12333 and12958; in National Security Directive 42; and in other applicable law. These authoritiesare reflected in DCID 1/1, *The Authorities and Responsibilities of the Director ofCentral Intelligence as Head of the U.S. Intelligence Community*.

A. Purpose

1. This directive establishes the security policy and procedures for storing, processing, and communicating classified intelligence information in information systems (ISs). For purposes of this Directive, *intelligence information* refers to Sensitive Compartmented Information and special access programs for intelligence under the purview of the DCI. An *information system* is any telecommunications and/or computer related equipment or interconnected system or subsystems of equipment that is used in the acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of voice and/or data (digital or analog); it includes software, firmware, and hardware.

2. Intelligence information constitutes an asset vital to the effective performance of our national security roles. It is essential that this information be properly managed, and that its confidentiality, integrity, and availability be ensured. Therefore, this policy and its implementation manual:

a. Provide policy and procedures for the security and protection of systems that create, process, store, and transmit intelligence information.

b Provide administrative and system security requirements, including those for interconnected systems.

c. Define and mandate the use of a risk management process.

d. Define and mandate the use of a certification and accreditation process.

e. Promote the use of efficient procedures and cost-effective, computer-based security features and assurances.

f. Describe the roles and responsibilities of the individuals who constitute the decision-making segment of the IS security community and its system users.

g. Require a life-cycle management approach to implementing system security requirements.

h. Introduce the concepts *Levels-of-Concern* and *Protection Level* of information.

B. Policy

1. Intelligence information *shall be appropriately safeguarded at all times*, including when used in information systems. The information systems shall be protected. Safeguards shall be applied such that (1) individuals *are held accountable for their actions*; (2) information *is accessed only by authorized individuals* and processes*; (3) information is *used only for its authorized purpose(s);* (4) information *retains its content integrity*; (5) information *is available to satisfy mission requirements*; and (6) information *is appropriately marked and labeled.*

[**Authorized individuals* are those with the appropriate clearance, formal access approvals, and need-to-know.]

2. Appropriate security measures shall be implemented to ensure the *confidentiality, integrity, and availability* of that information. The mix of security safeguards selected for systems that process intelligence information shall ensure that the system meets the policy requirements set forth in this policy and its implementation manual.

a. Information systems security shall be an integral part of all system life-cycle phases for all systems.

b. The security of systems shall be reviewed whenever changes occur to missions, information systems, security requirements, or threat, and whenever there are significant adverse changes to system vulnerabilities.

c. Appropriate authorities, as defined in the Manual, shall be immediately notified of any threats or vulnerabilities impacting systems that process their data.

d. All ISs are subject to monitoring consistent with applicable laws and regulations, and as provided for by agency policies, procedures, and practices. As a minimum, monitoring will assess the adequacy of the confidentiality, integrity, and availability controls.

3. All systems shall be certified> and accredited in compliance with the requirements stated in the associated implementation manual and following the direction and guidance provided in the Designated Accrediting Authority (DAA)-approved certification and accreditation (C&A) process. C&A is a comprehensive process to ensure implementation of security measures that effectively counter relevant threats and vulnerabilities. C&A consists of several iterative,

interdependent phases and steps whose scope and specific activities vary with the IS being certified and accredited.

a. A risk assessment shall be performed for each IS to identify specific areas that require safeguards against deliberate or inadvertent unauthorized disclosure, modification, or destruction of information; denial of service; and unauthorized use of the IS. Countermeasures shall be applied in those areas to eliminate or adequately reduce the identified risk. The risk assessment shall be based on the accompanying manual, input from the organization's counterintelligence (CI) component, the organization's mission requirements, the classification and sensitivity of the information, and a balanced, cost-effective application of security disciplines and technologies. These security disciplines include, but are not limited to, information systems security, operations and administrative security, personnel security, physical security, and communications security.

b. Systems shall be reviewed for compliance with the policy and its implementation manual and the security documents derived from the manual.

c. In support of the C&A process, the DCI shall establish and maintain a formal information security education, awareness and training program. The agencies, departments, and components covered by this policy, including those to which accrediting authority is delegated, will establish similar programs, as well as accreditation programs.

4. Each of the Principal Accrediting Authorities (PAAs) for the intelligence community may provide *one* annex to the implementation manual for their respective communities. The annex may be used only to provide clarification. Annexes are due not later than six months after the effective date of the manual. The Community Management Staff will review and coordinate the proposed annexes. The affected PAAs will submit any challenges or objections to the content of specific intelligence community annexes that they cannot resolve to the Community Management Staff for final resolution.

C. Responsibilities

1. In furtherance of the responsibilities of the DCI to ensure the protection of intelligence sources and methods, the Deputy Director of Central Intelligence for Community Management (DDCI/CM) shall ensure that the security requirements of this policy are implemented and that the associated manual is developed.

2. The DDCI/CM shall ensure that this Policy is reviewed biennially and that its associated Manual is reviewed as required to determine whether the threat environment, changes in technology, or any other factors require changes to one or both documents. To support these reviews, PAAs/DAAs will provide comments to the Community Management Staff for coordination. Individuals wishing to make comments may do so by sending them to the appropriate PAA/DAA for review and possible forwarding.

a. The DDCI/CM shall require the PAAs to plan, budget, allocate, and spend adequate resources to meet the security requirements specified by this directive.

b. The DDCI/CM shall review any unresolved conflicts related to this policy and the associated manual and will either attain agreed-to resolution of them by all affected parties or forward them with recommendations for resolution to the DCI.

3. For intelligence data, the designated Principal Accrediting Authorities with responsibility for all intelligence systems that are within their respective purviews arethe DCI, EXDIR/CIA, AS/DOS (Intelligence & Research), DIRNSA, DIRDIA, ADIC/FBI (National Security Div), D/Office of Intelligence/DOE, SAS/Treasury (National Security), D/NIMA, and the D/NRO.

a. Systems processing intelligence information that operate at Protection Levels 4 or 5, and all components of such systems, shall be accredited only by the Director of the National Security Agency (DIRNSA), the Director of the Defense Intelligence Agency (DIRDIA), the Director of the National Reconnaissance Office (D/NRO), or the Executive Director of the Central Intelligence Agency (EXDIR/CIA). Only the DCI may further delegate the authority to accredit these systems.

b. NFIB members may delegate, to the extent they consider appropriate, their authority to accredit systems processing intelligence information or components of such systems that operate at Protection Levels 1, 2, or 3. But they retain ultimate responsibility for the security of the information processed in those systems.

4. The PAA shall ensure the establishment of an information systems security incident response and reporting capability that detects incidents, establishes a trained response element, maintains statistics, initiates an investigation, and recovers operational capability for the information.

D. Applicability

1. This policy and its associated implementation manual apply to all United States government organizations', their commercial contractors', and Allied governments' ISs that process, store, or communicate intelligence information.*

[*See the definition of *intelligence information* in sec. E, below.]

2. Nothing in this policy or the associated manual supersedes the requirements of the Atomic Energy Act of 1954, as amended (Chapter II, Public Law 585), for the control, use, and dissemination of Restricted Data or Formerly Restricted Data.

3. Nothing in this policy or the associated manual supersedes any statutory or Presidential requirement for the handling of cryptologic data or Communications Security (COMSEC)-related material.

4. This policy supersedes the policy in Directive of Central Intelligence Directive 1/16, July 1988.

5. This directive is effective for five years from the date of implementation. At that time, it shall be reviewed for continued applicability.

E. Definitions

This listing defines key terms relative to information systems securitypolicy.

Accreditation

The official management decision to permit operation of an IS in a specified environment at an acceptable level of risk, based on the implementation of an approved set of technical, managerial, and procedural safeguards.

Availability

Timely, reliable access to data and information services for authorized users.

Certification

The comprehensive evaluation of the technical and non-technical security features of an IS and other safeguards, made as part of and in support of the accreditation process, to establish the extent to which a particular design and implementation meet a specified set of security requirements.

Clearance

Formal certification of authorization to have access to classified information other than that protected in a special access program (including SCI). Clearances are of three types: confidential, secret, and top secret. A top secret clearance permits access to top secret, secret, and confidential material; a secret clearance, to secret and confidential material; and a confidential clearance, to confidential material.

Confidentiality

Assurance that information is not disclosed to unauthorized entities or processes.

Cryptanalysis

Operations performed in converting encrypted messages to plain text without initial knowledge of the cryptoalgorithm and/or key employed in the encryption.

Cryptography

Art or science concerning the principles, means, and methods for rendering plain information unintelligible and for restoring encrypted information to intelligible form.

Cryptologic Data

Information relating to cryptography and cryptanalysis.

Designated Accreditation Authority (DAA)

The official with the authority to formally assume responsibility for operating a system at an acceptable level of risk.

Formal Access Approval

Documented approval by a Data Owner to allow access to a particular category of information. Such access generally requires signing of an appropriate non-disclosure agreement, and entry of the individual's name on an access roster. For intelligence information, formal access approval is indicated by the requirement for signing an "Intelligence Non-Disclosure Agreement."

Information

The intelligence derived from the data on or about a system, or the intelligence obtained from the structure or organization of that data.

Information System (IS)

Any telecommunications and/or computer related equipment or interconnected system or subsystems of equipment that is used in the acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of voice and/or data (digital or analog); includes software, firmware, and hardware.

Integrity

Protection against unauthorized modification or destruction of information.

Intelligence Information

For purposes of this Directive, *intelligence information* refers to Sensitive Compartmented Information and special access programs for intelligence under the purview of the DCI..

Level-of-Concern

A rating assigned to an IS by the DAA. A separate Level-of-Concern is assigned to each IS for confidentiality, integrity, and availability. The Level-of-Concern for confidentiality, integrity, and availability can be Basic, Medium, or High. The Level-of-Concern assigned to an IS for confidentiality is based on the sensitivity of the information it maintains, processes, and transmits. The Level-of-Concern assigned to an IS for integrity is based on the degree of resistance to unauthorized modifications. The Level-of-Concern assigned to an IS for availability is based on the needed availability of the information maintained, processed and transmitted by the system for mission accomplishment, and how much tolerance for delay is allowed.

Need-to-Know

A determination made by an authorized holder of classified information that a prospective recipient of information requires access to specific classified information in order to perform or assist in a lawful and authorized governmental function.

Principal Accrediting Authority (PAA)

The senior official having the authority and responsibility for all intelligence systems within an agency. Within the Intelligence Community, the PAAs are the DCI, EXDIR/CIA, AS/DOS (Intelligence & Research), DIRNSA, DIRDIA, ADIC/FBI (National Security Div), D/Office of Intelligence/DOE, SAS/Treasury (National Security), D/NIMA, and the D/NRO.

Processing

The state that exists when information is being accessed or acted-upon by one or more steps proceeding in a predetermined sequence or method.

Protection Level

An indication of the implicit level of trust that is placed in a system's technical capabilities. A Protection Level is based on the classification and sensitivity of information processed on the system relative to the clearance(s), formal access approval(s), and need-to-know of all direct and indirect users that receive information from the IS without manual intervention and reliable human review. Protection Levels replace modes of operation defined in the 1988 DCID 1/16.

Restricted Data (RD)

All data concerning the following, but not including data declassified or removed from the RD category pursuant to section 142 of the Atomic Energy Act:

(1) Design, manufacture, or utilization of atomic weapons;

(2) Production of special nuclear material; or

(3) Use of special nuclear material in the production of energy.

Risk

The expected loss from a given attack or incident. For an attack/defense scenario, risk is assessed as a combination of *threat* (expressed as the probability that a given action, attack or incident will occur, but may also be expressed as frequency of occurrence), *vulnerability* (expressed as the probability that the given action, attack, or incident will succeed, given that the action, attack or incident occurs) and *consequence* (expressed as some measure of loss, such as dollar cost, resources cost, programmatic impact, etc.). The total risk of operating a system is assessed as a combination of the risks associated with all possible threat scenarios. Risk is reduced by countermeasures.

Security Incident

An act or circumstance in which there is a deviation from the requirements of the governing security regulations. Compromise, inadvertent disclosure, need-to-know violation, and administrative deviation are examples of security incidents.

Sensitive Compartmented Information

Classified information concerning or derived from intelligence sources, methods, or analytical processes, which is required to be handled within formal access control systems established by the Director of Central Intelligence (DCID 1/19).

Special Access Program (SAP)

A program established for a specific class of classified information that imposes safeguarding and access requirements that exceed those normally required for information at the same classification level (EO 12958).

System

An Information System (IS).

Threat

Any circumstance or event with the potential to cause harm to an information system in the form of destruction, disclosure, adverse modification of data, and/or denial of service.

Vulnerability

A weakness in an IS, or cryptographic system, or component (e.g., system security procedures, hardware design, internal controls) that could be exploited.

This policy is complemented by *Protecting Sensitive CompartmentedInformation within Information Systems (DCID 6/3)—Manual*.

DIRECTOR OF CENTRAL INTELLIGENCE — 5 June 1999 DATE