SECRET/[redacted]

Director of Central Intelligence Directive 6/5: Policy for the Protection of Certain non-SCI Sources and Methods Information (SAMI)
(Signed 12 February 2001)

[redacted] Pursuant to the National Security Act of 1947, as amended, Executive Orders 12333 and 12958, and other applicable law and directives, the Director of Central Intelligence (DCI) promulgates this directive for the protection of certain intelligence sources and methods. Applicable provisions cited in DCID 1/1 (19 November 1998) are included by reference.

A. [redacted] Purpose

1. [redacted] This Directive establishes the DCI's security policy and procedures for storing, processing, and communicating any classified non-SCI Sources and Methods Information (SAMI) that has been determined by the Data Owner to need the protection afforded by this Directive. This DCID and its Implementation Manual enable the Intelligence Community (IC) to share information more extensively under appropriate controls

[redacted]

2. [redacted] For purposes of this Directive, SAMI refers to classified sources and methods information that is not protected within a Sensitive Compartmented Information (SCI) control system or any other Special Access Program (SAP), but that is subject to countermeasures and requires need-to-know protections. Nothing in this Directive is intended to modify the authorities and responsibilities established by applicable law or directive to protect intelligence sources and methods not marked as SAMI pursuant to this Directive, or the authorities of the heads of executive departments and agencies to exercise, consistent with the authorities and responsibilities of the DCI, their authorities to manage elements of the IC within their departments.

3. [redacted] This policy Directive and its Implementation Manual, which will be consistent with the

(2) (b)(1) (b)(3)

purpose, processes, and procedures set forth in this Directive:

a. Establish SAMI as a category of intelligence information requiring a specific dissemination marking and related protections, as described in this DCID.

b. Provide policy and procedures for securely protecting information systems (IS) that create, process, store, and transmit SAMI information.

c. Include [redacted] requirements for protecting SAMI, including those for interconnected systems.

d. Mandate the use of a risk management process.

e. Describe the roles and responsibilities of the individuals who constitute the decisionmaking segment for providing the approval to operate systems processing SAMI.

f. [redacted]

B. [redacted] Policy

1. [redacted] This directive encourages the use of SAMI management controls as appropriate to maximize the dissemination of intelligence without the need for more restrictive caveats. Data Owners or their designee(s) shall determine, at their discretion and consistent with this Directive, whether their classified non-SCI sources and methods intelligence information needs the protection afforded by this Directive. All information needing such protection shall be marked as SAMI and be in accordance with DCID 1/7 and the Classification and Control Marking Register.[1] This directive does not address sources and methods intelligence information that is not marked as SAMI by its originator.

[1] Per Executive Order 12958, if all portions contain SAMI, as well as the other header and footer markings, then the statement "ALL PORTIONS MARKED..." may be used in the body of the document.

2. SAMI controls are applicable to both manual and electronic handling of information. No special protections, other than classification and dissemination markings, are required for non-electronic SAMI products, since standard need-to-know protections apply and are adequate. However, SAMI markings must be maintained to ensure continuous enforcement of need-to-know handling controls and protections.

C. SAMI Procedures

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

2. *SAMI Categories.* In order to be considered eligible for protection as SAMI, information must fall within one of the categories of non-SCI intelligence information presented in this paragraph unless otherwise provided by the DCI. The DCI may approve protection as SAMI any other types of information that are classified as non-SCI sources and methods intelligence information.

a.

b.

c.

d.

e.

f.

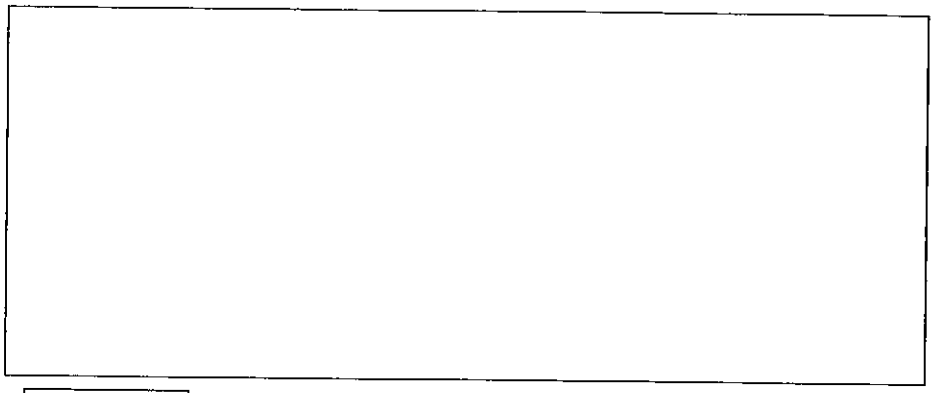
g.

h.

i.

j.

k.



3. [redacted] *Security and Need-to-Know.* Data owners shall implement appropriate security measures to ensure the *confidentiality, integrity, and availability* of SAMI. The combination of security safeguards selected for systems that process SAMI shall ensure that the information is provided only to authorized individuals with a valid need-to-know. SAMI may be stored and accessed:

a. [redacted]

b. [redacted]

c. [redacted]

4. [redacted] *Approved Need-to-Know.* Supervisors must validate their employees' need-to-know for SAMI, [redacted]

5. [redacted] *Certification and Accreditation.*

a. All ISs that process SAMI shall be certified and accredited by the Designated Approving/Accrediting Authority (DAA) or designee in compliance with appropriate National, DoD, and IC policies and procedures (e.g., DoD Instruction 5200.40--the DoD Information Technology Security Certification and Accreditation Process (DITSCAP), DCID 6/3, etc.). Certification and Accreditation

(C&A) is a comprehensive process to ensure implementation of security measures that effectively counter relevant threats and vulnerabilities.

b. As part of the C&A process, 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. As required by the DAA or Data Owner, countermeasures shall be applied in those areas to reduce the identified risk to an acceptable level.

c. ISs processing SAMI shall be reviewed and reaccredited by the DAA or designee [redacted]

d. Cognizant DAAs and Data Owners shall be immediately notified of any threats or vulnerabilities affecting systems that process SAMI.

e. All ISs that process SAMI are subject to [redacted] consistent with this Directive; applicable laws and regulations; and as provided for by government policies, procedures, and practices. As a minimum, [redacted]

6. [redacted] *Marking and Use of SAMI*. Within a document containing a SAMI dissemination marking, the designated portion marking will be used on those portions containing SAMI. To exploit information marked SAMI to its fullest potential, SAMI products may be sanitized for dissemination after deliberately disguising or removing the uniquely sensitive aspects of the original material in accordance with DCID 1/7. Sanitization permits access to the needed information at the level at which it will be most useful while ensuring the protection of sensitive sources and operational methods. SAMI sanitization rules

do not supersede the requirements to obtain originator approval for further dissemination of ORCON or NOFORN. Sanitization procedures are set forth in the Implementation Manual.

7. [redacted] *Designated Intelligence Disclosure Officials (DIDOs).* DIDOs may exercise their authorities for authorized disclosure or release of SAMI to [redacted] through established channels in accordance with DCID 1/7, DCID 5/6, and NDP-1 to the extent consistent with DCIDs and other DCI guidance.

D. [redacted] Responsibilities

1. [redacted] **Data Owner**: The Data Owner or Designee(s) shall:

a. Determine if their information shall be marked as SAMI.

b. Provide instruction to the DAA concerning the sensitivity of information under the Data Owner's purview to assist in the DAA's decision regarding the security protections needed [redacted]

c. Revoke permission to process the information on any information system if unsatisfied with the protections it provides, and formally notify the DAA of any decision to revoke.

2. [redacted] The Data Owner or the DIDO shall determine a [redacted] need-to-know for his/her organization's SAMI.

3. [redacted] **DAA**: The DAA shall:

a. Grant formal accreditation to operate a system processing SAMI. The DAA has the authority to withdraw accreditation, suspend operations, grant interim approval to operate, or grant variances when circumstances warrant. [redacted]

DAAs are responsible and accountable for the security of the SAMI processed on the ISs they accredit.

b.

4. **Supervisor**: Supervisors shall validate their employees' need-to-know for SAMI,

E. Applicability

1. This Directive applies to all United States Government organizations and their commercial contractors whose information systems process, store, or communicate information marked and protected as SAMI.

2. This Directive does not apply to foreign-owned and -operated information systems. SAMI will be sanitized in accordance with this DCID and the Implementation Manual prior to release.

3. Nothing in this Directive supersedes the requirements of Executive Order 12958, Classified National Security Information.

4.

F. Violations and Reporting Requirements

Senior Officials of the Intelligence Community (SOICs) shall ensure that the DCI is immediately apprised of significant violations of safeguards or other incidents indicating or confirming compromise of SAMI. The DCI must be promptly informed so that appropriate IC coordination and action can occur.

G. Reference

1. National Security Act of 1947, as amended.

2. National Security Directive 42, National Policy for the Security of National Security Telecommunications and Information Systems, dated 5 July 1990.

3. Executive order 12333, United States Intelligence Activities, dated 4 December 1981.

4. Executive Order 12958, Classified National Security Information, dated 17 April 1995.

5. DCID 1/1, The Authorities and Responsibilities of the Director of Central Intelligence as Head of the U.S. Intelligence Community, dated 19 November 1998.

6. DCID 1/7, Security Controls on the Dissemination of Intelligence Information, 30 June 1998.

7. DCID 1/21, Physical Security Standards for Sensitive Compartmented Information Facilities, 29 July 1994.

8. DCID 5/6, Intelligence Disclosure Policy, dated 30 June 1998.

9. DCID 6/3, Protecting Sensitive Compartmented Information within Information Systems, dated 5 Jun 99.

10. NDP-1, National Policy and Procedures for the Disclosure of Classified Military Information to Foreign Governments and International Organizations (Short Title: National Disclosure Policy), 1 October 1988.

11. DoD 5200.1-R, DoD Information Security Program, January 1997

12. DoD Directive 5200.5, Communications Security (COMSEC), dated 21 April 1990.

13. DoD Directive 5200-28, Security Requirements for Automated Information Systems (AISs), dated 21 March 1988.

SECRET/

14. DoD Instruction 5200.40, DoD Information Technology Security Certification and Accreditation (C&A) Process (DISTCAP), dated 30 December 1997.

Director of Central Intelligence Date

SECRET/[redacted]

Attachment

[redacted] **Glossary of Terms**

This attachment shall be incorporated into standard operating procedures to be published separately. (See the SAMI Implementation Manual.)

Accountability	The property that allows auditing of information system activities to be traced to persons or processes that may then be held responsible for their actions.
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.
Administrative Security	The management constraints, operational, administrative, and accountability procedures and supporting control established to provide an acceptable level of protection for data.
Attack	Attempt to gain unauthorized access to an IS's services, resources, or information, or the attempt to compromise an IS's integrity, availability, or confidentiality.
Audit Trail	A chronological record of system activities that is sufficient to enable the reconstruction, reviewing, and examination of the sequence of environments and activities surrounding or leading to an operation, a procedure, or an event in a transaction from its inception to final results.
Authenticator	Means used to confirm the identity of a station (e.g., device, workstation, server, router, etc.), originator, individual or process. For example, a

password is often used to authenticate the individual using a particular user identifier.

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

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.
Configuration Management	The management of security features and assurances through control of changes made to a system's hardware, software, firmware, documentation, test, test fixtures and test documentation throughout the development and operational life of the system.
Countermeasure	Any action, device, procedure, technique, or other measure that reduces the vulnerability of or threat to a system.
Controlled Interface	A mechanism that facilitates the adjudication of different interconnected system security policies (e.g., controlling the flow of information into or out of an interconnected system).
Counter-intelligence	That phase of intelligence covering all activity devoted to neutralizing the effectiveness of hostile foreign intelligence collection activities.
Cryptography	Art or science concerning the principles, means, and methods for rendering plain information unintelligible and for restoring encrypted information to intelligible form.
Data Owner	The IC organization that has final legal authority for specified information.

Data Sanitization	The removal, paraphrasing, synthesizing with other information, or otherwise disguising all references or terminology that will reveal or relate the material to sensitive source, method, targeting, content, event, or situation information.
Designated Accrediting Authority (DAA)	IC title for the official with the authority to formally assume responsibility for operating a system at an acceptable level of risk. This is synonymous with Designated Approving Authority.
Designated Approving Authority (DAA)	Official with the authority to formally assume responsibility for operating a system at an acceptable level of risk. This term is synonymous with Designated Accrediting Authority and Delegated Accrediting Authority.
Designated Intelligence Disclosure Officials (DIDOs)	The heads of departments or agencies with organizations in the Intelligence Community or the heads of such organizations, and their specifically designated subordinates whose names and positions are certified to the DCI in writing, and other US officials designated by the DCI, with authority to approve or deny disclosure or release of uncaveated intelligence information to foreign governments in accordance with applicable disclosure policies and procedures.
Direct Interface	A connection between networks without any intervening processor(s) (e.g., firewall, guard, etc.) that protects and controls the connection.
Discretionary Access Control (DAC)	A means of restricting access to objects (e.g., files, data entities) based on the identity and need-to-know of subjects (e.g., users, processes) and/or groups to which the object belongs. The controls are discretionary in the sense that a subject with a certain access permission

	is capable of passing that permission (perhaps indirectly) on to any other subject (unless restrained by mandatory access control).
Foreign Nationals	Individuals who are not United States citizens.
Indirect Interface	An electronic connection between networks with an intervening processor(s) (e.g., firewall, guard, etc.) that protects and controls the connection.
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.
Information System Security Manager (ISSM)	The manager responsible for an organization's information system security program.
Information System Security Officer (ISSO)	The person responsible to the ISSM for ensuring that security is maintained for a specific IS. Sometimes referred to as a Network Security Officer or System Security Officer.
Integrity	Quality of an IS reflecting the logical correctness and reliability of the operating system; the logical completeness of the hardware and software implementing the protection mechanisms; and the consistency of the data structures and occurrence of the stored data. Note that, in a formal security mode, integrity is interpreted more narrowly to mean protection against unauthorized modification or destruction of information.

Interconnected System	A set of separately-accredited or managed systems that are connected together.
Malicious Code	Software or firmware that is designed with the intent of having some adverse impact on the confidentiality, integrity, or availability of an IS.
Media	All forms of storage (e.g., optical media, disks, memory, or paper output).
Media Sanitization	The removal of information from media or equipment such that data recovery using any known technique or analysis is prevented, as well as the removal of all classified labels and markings.
Memorandum of Agreement (MOA)	A written agreement among the DAAs responsible for the information processed and maintained by an IS (or collection of ISs), or between a DAA and a Data Owner. The MOA stipulates all of the terms and conditions of the security arrangements that will govern the operation of the IS(s). The MOA shall include at least: (1) a general description of the information to be offered by each participating DAA and/or Data Owner; and (2) a discussion of all of the security details pertinent to the exchange of information between the DAAs. In addition, where the MOA is to cover an interconnected network of ISs under the purview of different DAAs, then the MOA shall also include a description of the types of information services each participating IS will provide, and identify a lead DAA. If no lead DAA is named, then both parties share responsibility.
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.

Non-Repudiation	Assurance the sender of data is provided with proof of delivery and the recipient is provided with proof of the sender's identity, so neither can later deny having processed the data.
Object	A passive entity that contains or receives information. Access to an object potentially implies access to the information that it contains.
Procedural Security	The management constraints, operational, administrative, and accountability procedures, and supplemental controls established to provide protection for sensitive information.
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.
Records Management	The policy for the tagging of information for records keeping requirements as mandated in the Federal Records Act and the National Archival and Records Requirements.
Remote Access	Any communication over a non-direct data link, including internets, intranets, client-server LANs, telephone lines, etc.
Remote Diagnostics Maintenance	The operational procedure that involves connection of a system to an external (i.e., outside of the facility securing the system) remote service for analysis or maintenance.
Responsible Official	Operationally, the responsible official makes decisions regarding protection of the Data Owner's information within the responsible official's agency. The individual who has final statutory or operational responsibility for establishing protection requirements for a given piece of information within the

responsible official's agency.

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.

Risk Assessment

The process of analyzing the threats to and vulnerabilities of an information system, analyzing the potential impact that the loss of information or capabilities of a system would have on national security, and, based upon these analyses, identifying appropriate and cost-effective countermeasures.

Risk Management

The discipline of identifying and measuring security risks associated with an IS, and controlling and reducing those risks to an acceptable level.

Security-Related Event

Security-related events include any event that would cause a deleterious change in the system or its environment, and any event that an experienced Information System Security Officer (ISSO) would consider to require noting, investigating, or preventing (e.g., the discovery of malicious code in an IS, the discovery of an attempt to introduce malicious code into an IS). Security-related events also include inadvertent disclosures, and changes to missions,

	information systems, security requirements, user population (e.g., clearance level or nationality), threat environment, or adverse changes to system vulnerabilities.
Security Markings	Indicators applied to a document, storage media, or hardware component to designate categorization and handling restrictions applicable to the information in the document.
Storage	The state that exists when information is being held for use until needed for processing.
Strong Authentication	A form of authentication whereby it is very difficult or impossible for a hostile user to successfully intercept and employ a transmitted authenticator.
Supervisor	An appropriately-cleared individual who serves in a management role, and has supervisory responsibilities for individuals who require SAMI access in order to perform or assist in a lawful and authorized governmental function.
System Security Authorization Agreement (SSAA)	A document that describes the agreement among the DAA(s), the Certification Authority, the system user representative, and the program manager. It is used to guide actions, document decisions, specify requirements, document certification tailoring and level-of-effort, identify potential solutions, and maintain operational systems security.
System Security Plan (SSP)	A formal document describing the planned operating conditions of the system and the expected residual risk of operating the system.
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.

Transmission	The state that exists when information is being sent from one location to one or more other locations.
User	An individual who can receive information from, input information to, or modify information on, a system without a reliable human review. A user electronically connects to an IS (typically via an interactive link); user access is automatically limited in real-time by the IS on some basis (e.g., security clearance or need-to-know). It is often convenient to refer to a user who is NOT a privileged user as a General User or Authorized User.
Vulnerability	Weakness in an IS, system security procedures, internal controls, or implementation that could be exploited.