



---

# **Director of Central Intelligence Directive 1/7(1)**

## **Security Controls on the Dissemination of Intelligence Information**

(Effective 30 June 1998)

### **Introduction**

Pursuant to the provisions of the National Security Act of 1947, as amended, Executive Order 12333, Executive Order 12958 and implementing directives thereto, policies, controls, and procedures for the dissemination and use of intelligence information and related materials are herewith established in this Director of Central Intelligence Directive (Directive or DCID). Nothing in this policy is intended to amend, modify, or derogate the authorities of the DCI contained in Statute or Executive Order.

### **1.0 Policy**

1.1 It is the policy of the DCI that intelligence be produced in a way that balances the need for maximum utility of the information to the intended recipient with protection of intelligence sources and methods. The controls and procedures established by this directive should be applied uniformly in the dissemination and use of intelligence originated by all Intelligence Community components in

accordance with the following principles:

1.1.1 Originators of classified intelligence information should write for the consumer. This policy is intended to provide for the optimum dissemination of timely, tailored intelligence to consumers in a form that allows use of the information to support all need to know customers.

1.1.2 The originator of intelligence is responsible for determining the appropriate level of protection prescribed by classification and dissemination policy. Originators shall take a risk management approach when preparing information for dissemination.

## 2.0 Purpose

2.1 This Directive establishes policies, controls, and procedures for the dissemination and use of intelligence information to ensure that, while facilitating its interchange for intelligence purposes, it will be adequately protected. This Directive implements and amplifies applicable portions of the directives of the Information Security Oversight Office issued pursuant to Executive Order 12958 (E.O.) and directives of the Security Policy Board issued pursuant to E.O. 12958 and PDD-29.

2.2 Additionally, this Directive sets forth policies and procedures governing the release of intelligence to contractors and consultants, foreign governments, international organizations or coalition partners consisting of sovereign states, and to foreign nationals and immigrant aliens, including those employed by the US Government.

2.3 Executive Order 12958 provides for the establishment of Special Access Programs, including Sensitive Compartmented Information. DCID 3/29 provides procedures for the establishment and review of Special Access Programs

pertaining to intelligence activities and restricted collateral information. Intelligence Community components may establish and maintain dissemination controls on such information as approved under the policies and procedures contained in DCID 3/29, this DCID, and implementing guidance.

### 3.0 Definitions

3.1 "Caveated" information is information subject to one of the authorized control markings under Section 9.

3.2 Intelligence Community (and agencies within the Intelligence Community) refers to the United States Government agencies and organizations and activities identified in section 3 of the National Security Act of 1947, as amended, 50 USC 401a(4), and Section 3.4(f) (1 through 6) of Executive Order 12333.

3.3 Intelligence information and related materials (hereinafter referred to as "Intelligence") include the following information, whether written or in any other medium, classified pursuant to E.O. 12958 or any predecessor or successor Executive Order:

3.3.1 Foreign intelligence and counterintelligence defined in the National Security Act of 1947, as amended, and in Executive Order 12333:

3.3.2 Information describing US foreign intelligence and counterintelligence activities, sources, methods, equipment, or methodology used for the acquisition, processing, or exploitation of such intelligence; foreign military hardware obtained through intelligence activities for exploitation and the results of the exploitation; and any other data resulting from US intelligence collection efforts; and,

3.3.3 Information on Intelligence Community protective security programs (e.g., personnel, physical, technical, and information security).

3.4 "Need-to-know" is the determination by an authorized holder of classified information that a prospective recipient requires access to specific classified information in order to perform or assist in a lawful and authorized governmental function. Such persons shall possess an appropriate security clearance and access approval granted pursuant to Executive Order 12968, Access to Classified Information.

3.5 Senior Official of the Intelligence Community (SOIC) is the head of an agency, office, bureau, other intelligence element as identified in Section 3 of the National Security Act of 1947, as amended, 50 USC 401a(4), and Section 3.4(f) (1 through 6) of Executive Order 12333.

3.6 A "tear line" is the place on an intelligence report (usually denoted by a series of dashes) at which the sanitized version of a more highly classified and/or controlled report begins. The sanitized information below the tear line should contain the substance of the information above the tear line, but without identifying the sensitive sources and methods. This will permit wider dissemination, in accordance with the "need to know" principle and foreign disclosure guidelines, of the information below the tear line.

#### 4.0 General Applicability

4.1 In support of the Policy Statement in Section 1.0, classifiers of intelligence information shall take a risk management approach when preparing information for dissemination. In the interest of the widest possible dissemination of information to consumers with a "need to know," classifiers shall carefully consider the needs of all appropriate intelligence consumers regarding sources and methods information or sensitive analytic comments and use

control markings only when necessary and in accordance with this directive, using tearlines and other formats to meet consumer needs for intelligence.

4.2 In carrying out this policy, intelligence producers shall prepare their reports and products at the lowest classification level commensurate with expected damage that could be caused by unauthorized disclosure. When necessary, the material should be prepared in other formats (e.g. tear-line form) to permit broader dissemination or release of information.

4.3 All material shall be portion marked to allow ready identification of information that cannot be broadly disseminated or released, except for material for which a waiver has been obtained under EO 12958.

4.4 The substance of this Directive shall be promulgated by each Intelligence Community component, and appropriate procedures permitting prompt interagency consultation established.

## 5.0 Use By and Dissemination Among Executive Branch Departments/Agencies of the US Government

5.1 Executive Order 12958 provides that classified information originating in one US department or agency shall not be disseminated beyond any recipient agency without the consent of the originating agency. However, to facilitate use and dissemination of intelligence within and among Intelligence Community components and to provide for the timely flow of intelligence to consumers, the following controlled relief to the "third agency rule" is hereby established:

5.1.1 Each Intelligence Community component consents to the use of its classified intelligence in classified intelligence

products of other Intelligence Community components, including its contractors under Section 6, and to the dissemination of those products within executive branch departments/agencies of the US Government, except as specifically restricted by controls defined in this directive or other DCI guidance.

5.1.2 As provided in 5.1.1, classified intelligence that bears no restrictive control markings may be given secondary US dissemination in classified channels to any US executive branch department/agency not on original distribution if (a) the intelligence has first been sanitized by the removal of all references and inferences to intelligence sources and methods and the identity of the producing agency, or (b) if the product is not so sanitized, the consent of the originator has been obtained. If there is any doubt concerning a reference or inference to intelligence sources and methods, relevant intelligence documents should not be given secondary dissemination until the recipient has consulted with the originator.

5.1.3 Any component disseminating intelligence beyond the Intelligence Community assumes responsibility for ensuring that recipient organizations agree to observe the need-to-know principle and the restrictions prescribed by this directive, and to maintain adequate safeguards.

## 6.0 Policy and Procedures Governing the Release of Intelligence to Contractors and Consultants

6.1 SOICs, or their designees, may release intelligence to appropriately cleared or access-approved US contractors and consultants (hereinafter "contractor") having a demonstrated "need to know" without referral to the originating agency prior to release provided that:

6.1.1 At the initiation of the contract, the SOIC or her/his designee specifies and certifies in writing that disclosure of

the specified information does not create an unfair competitive advantage for the contractor or a conflict of interest with the contractor's obligation to protect the information. If, during the course of the contract, the contractor's requirements for information changes to require new or significantly different information, the SOIC or his/her designee shall make a new specification and certification. In cases where the designated official cannot or does not resolve the issue of unfair competitive advantage or conflict of interest, consent of the originator is required;

6.1.2 Release is made only to contractors certified by the SOIC (or designee) of the sponsoring organization as performing classified services in support of a national security mission;

6.1.3 The contractor has an approved safeguarding capability if retention of the intelligence is required;

6.1.4 Contractors are not authorized to disclose further or release intelligence to any of their components or employees or to another contractor (including subcontractors) without the prior written notification and approval of the SOIC or his/her designee unless such disclosure or release is authorized in writing at the initiation of the contract as an operational requirement;

6.1.5 Intelligence released to contractors, all reproductions thereof, and all other material generated based on, or incorporating data therefrom (including authorized reproductions), remain the property of the US Government. Final disposition of intelligence information shall be governed by the sponsoring agency;

6.1.6 National Intelligence Estimates (NIEs), Special National Intelligence Estimates (SNIEs), and Interagency Intelligence Memoranda may be released to appropriately cleared contractors possessing an appropriate level facility

clearance and need-to-know, except as regulated by provisions concerning proprietary information as defined in sections 6.1.1.7 and 9.3, below;

6.1.7 Except as provided in section 6.3 below, intelligence that bears the control marking "CAUTION-PROPRIETARY INFORMATION INVOLVED" (abbreviated "PROPIN" or "PR") may not be released to contractors, unless prior permission has been obtained from the originator and those providing the intelligence to the originator. Intelligence that bears the control marking, "DISSEMINATION AND EXTRACTION OF INFORMATION CONTROLLED BY ORIGINATOR" (abbreviated "ORCON") may only be released to contractors within Government facilities. These control markings are further described under Sections 9.2 and 9.3, below; and

6.1.8 Authorized release to foreign nationals or foreign contractors is undertaken through established channels in accordance with sections 7 and 8, and DCID 5/6, Intelligence Disclosure Policy, and the National Policy and Procedures for the Disclosure of Classified Military Information to Foreign Governments and International Organizations (abbreviated title: National Disclosure Policy 1 or NDP 1) to the extent consistent with DCIDs and other DCI guidance.

## 6.2 Policies and Procedures for Contractors Inside Government Owned or Controlled Facilities

6.2.1 Contractors who perform duties inside a Government owned or controlled facility will follow the procedures and policies of that sponsoring Intelligence Community member in accordance with Section 6.1 of this directive.

## 6.3 Policies and Procedures for Contractors Outside Government Owned or Controlled Facilities

6.3.1 Contractors who perform duties outside of Government owned or controlled facilities will adhere to the following additional policies and procedures:

6.3.1.1 The SOIC of the sponsoring agency, or her/his designee, is responsible for ensuring that releases to contractors of intelligence marked ORCON and/or PROPIN are made only with the consent of the originating agency pursuant to this Directive and through established channels; (See Sections 9.2 and 9.3);

6.3.1.2 The sponsoring agency shall maintain a record of material released;

6.3.1.3 Contractors shall establish procedures to control all intelligence received, produced, and held by them in accordance with the provisions of the National Industrial Security Program Operating Manual. This will not impose internal receipt and document accountability requirements for internal traceability and audit purposes;

6.3.1.4 All reproductions and extractions of intelligence shall be classified, marked, and controlled in the same manner as the original(s);

6.3.1.5 Sensitive Compartmented Information released to contractors shall be controlled pursuant to the provisions of DCID 1/19, Security Policy for Sensitive Compartmented Information (SCI); and,

6.3.1.6 Sponsoring agencies shall delete any reference to the Central Intelligence Agency, the phrase "Directorate of Operations" and any of its components, the place acquired, the field number, the source description, and field dissemination from all CIA Directorate of Operations reports passed to contractors, unless prior approval to do otherwise is obtained from CIA.

## 7.0 Release to Foreign Governments, International Organizations, and Coalition Partners

7.1 It is the policy of the DCI that intelligence may be shared with foreign governments, and international organizations or coalition partners consisting of sovereign states to the extent such sharing promotes the interests of the United States, is consistent with US law, does not pose unreasonable risk to U.S. foreign policy or national defense, and is limited to a specific purpose and normally of limited duration. The release of intelligence to such entities is subject to this Directive, DCID 5/6, Intelligence Disclosure Policy, and NDP 1 to the extent consistent with DCIDs and other DCI guidance.

7.1.1 Intelligence Community elements shall restrict the information subject to control markings to the minimum necessary. If it is not possible to prepare the entire report at the collateral, uncaveated level, IC elements shall organize their intelligence reports and products to identify clearly information not authorized for release to foreign entities.

7.2 Intelligence information that bears no specific control marking may be released to foreign governments, international organizations, or coalition partners provided that:

7.2.1 A positive foreign disclosure decision is made by a designated intelligence disclosure official in accordance with procedures in DCID 5/6;

7.2.2 No reference is made to the originating agency or to the source of the documents on which the released product is based; and,

7.2.3 The source or manner of acquisition of the intelligence (including analytic judgments or techniques), and/or the

location where the intelligence was collected (if relevant to protect sources and methods) is not revealed and cannot be deduced in any manner.

7.3 RESTRICTED DATA and FORMERLY RESTRICTED DATA may only be released to foreign governments pursuant to an agreement for cooperation as required by Sections 123 and 144 of Public Law 585, Atomic Energy Act of 1954, as amended.

## 8.0 Dissemination to Non-Governmental Foreign Nationals or Foreign Contractors

8.1 It is the policy of the DCI that no classified intelligence will be shared with foreign nationals, foreign contractors, or international organizations not consisting of sovereign states, except in accordance with the provisions of this Section.

8.2 Intelligence, even though it bears no restrictive control markings, will not be released in any form to foreign nationals or immigrant aliens (including those employed by, used by, or integrated into the US Government) without the permission of the originator. In such cases where permission of the originator has been granted, the release must be in accordance with DCID 5/6, and the NDP 1 to the extent consistent with DCIDs and other DCI guidance.

8.3 Release of intelligence to a foreign contractor or company under contract to the US Government must be through the foreign government of the country which the contractor is representing, unless otherwise directed in government-to-government agreements or there is an appropriate US channel for release of the information. Provisions concerning release to foreign governments is contained in Section 7.0, above.

## 9.0 Authorized Control Markings

9.1 DCI policy is that the authorized control markings for intelligence information in this Section shall be individually assigned as prescribed by an original classification authority (OCA) or by officials designated by a SOIC and used in conjunction with security classifications and other markings specified by Executive Order 12958 and its implementing directive(s). Unless originator consent is obtained, these markings shall be carried forward to any new format or medium in which the same information is incorporated.

9.1.1 To the maximum extent possible, information assigned an authorized control marking shall not be combined with uncaveated information in such a way as to render the uncaveated information subject to the control marking. To fulfill the requirements of paragraph 9.6.1 below, SOICs shall establish procedures in implementing directives to expedite further dissemination of essential intelligence. Whenever possible, caveated intelligence information reports should include the identity and contact instructions of the organization authorized to approve further dissemination on a case-by-case basis.

## 9.2 "DISSEMINATION AND EXTRACTION OF INFORMATION CONTROLLED BY ORIGINATOR" (ORCON)

9.2.1 This marking (ORCON or abbreviated OC) may be used only on classified intelligence that clearly identifies or would reasonably permit ready identification of intelligence sources or methods that are particularly susceptible to countermeasures that would nullify or measurably reduce their effectiveness. It is used to enable the originator to maintain continuing knowledge and supervision of distribution of the intelligence beyond its original dissemination. This control marking may not be used when access to the intelligence information will reasonably be protected by use of its classification markings, i.e., CONFIDENTIAL, SECRET or TOP SECRET, or by use of

any other control markings specified herein or in other DCIDs. Requests for further dissemination of intelligence bearing this marking shall be reviewed in a timely manner.

9.2.2 Information bearing this marking may be disseminated within the headquarters<sup>2</sup> and specified subordinate elements of recipient organizations, including their contractors within Government facilities. This information may also be incorporated in whole or in part into other briefings or products, provided the briefing or intelligence product is presented or distributed only to original recipients of the information. Dissemination beyond headquarters and specified subordinate elements or to agencies other than the original recipients requires advance permission from the originator.

9.2.3 Information bearing this marking must not be used in taking investigative or legal action without the advance permission of the originator.

9.2.4 As ORCON is the most restrictive marking herein, agencies that originate intelligence will follow the procedures established in the classified DCID 1/7 Supplement, "Guidelines for Use of ORCON Caveat."

9.3 "CAUTION-PROPRIETARY INFORMATION INVOLVED" (PROPIN). This marking is used, with or without a security classification, to identify information provided by a commercial firm or private source under an express or implied understanding that the information will be protected as a proprietary trade secret or proprietary data believed to have actual or potential value.<sup>3</sup> This marking may be used on government proprietary information only when the government proprietary information can provide a contractor(s) an unfair advantage, such as US Government budget or financial information. Information bearing this marking shall not be disseminated outside the Federal Government in any form without the express permission of

the originator of the intelligence and provider of the proprietary information. This marking precludes dissemination to contractors irrespective of their status to, or within, the US Government without the authorization of the originator of the intelligence and provider of the information. This marking shall be abbreviated "PROPIN" or "PR."

9.4 "NOT RELEASABLE TO FOREIGN NATIONALS" - NOFORM (NF). This marking is used to identify intelligence which an originator has determined falls under the criteria of DCID 5/6, "Intelligence Which May Not Be Disclosed or Released," and may not be provided in any form to foreign governments, international organizations, coalition partners, foreign nationals, or immigrant aliens without originator approval.

9.5 "AUTHORIZED FOR RELEASE TO ... (name of country(ies)/international organization)" (REL TO). This control marking is used when a limited exception to the marking requirements in Section 9.4 may be authorized to release the information beyond US recipients. This marking is authorized only when the originator has an intelligence sharing arrangement or relationship with a foreign government approved in accordance with DCI policies and procedures that permits the release of the specific intelligence information to that foreign government, but to no other in any form without originator consent.

#### 9.6 Further Dissemination of Intelligence with Authorized Control Marking(s)

9.6.1 This Directive does not restrict an authorized recipient of intelligence at any level from directly contacting the originator of the intelligence to ask for relief from a specific control marking(s) in order to further disseminate intelligence material to additional users for which the authorized original recipient believes there is a valid need-to-know. Authorized recipients are encouraged to seek such further dissemination

through normal liaison channels for release to US Government agencies or contractors and through foreign disclosure channels for foreign release, on a case-by-case basis, in order to expedite further dissemination of essential intelligence.

9.6.2 Authorized recipients may obtain information regarding points of contact at agencies that originate intelligence from their local dissemination authorities or from instructions issued periodically by these intelligence producers. Intelligence products often also carry a point of contact name/office and telephone number responsible for the product. If no other information is available, authorized recipients are encouraged to contact the producing agency of the document to identify the official or office authorized to provide relief from authorized control marking(s).

9.6.3 If there are any questions about whom to contact for guidance, recipients are also encouraged to contact the Director of Central intelligence (DCI) representative at the Commander-in-Chief (CINC) Headquarters, overseas mission, trade delegation, or treaty negotiating team under which they operate.

9.7 A SOIC may authorize the use of additional security control markings for Sensitive Compartmented Information (SCI), Special Access Program (SAP) information, restricted collateral information, or other classified intelligence information, consistent with policies and procedures contained in DCID 3/29 and this directive. A uniform list of security control markings authorized for dissemination of classified information by components of the Intelligence Community, and the authorized abbreviated forms of such markings, shall be compiled in the central register maintained pursuant to DCID 3/29. The forms of the markings and abbreviations listed in this register shall be the only forms of those markings used for dissemination of classified information by components of the Intelligence Community,

unless an exception is specifically authorized by a SOIC.

## 10.0 Dissemination and Disclosure Under Emergency Conditions

10.1 Certain emergency situations<sup>4</sup> that involve an imminent threat to life or mission warrant dissemination of intelligence to organizations and individuals not routinely included in such dissemination. When the national command authority (NCA) directs that an emergency situation exists, SOICs will ensure that intelligence support provided to the ongoing operations conforms with this Directive, DCID 5/6, and NDP 1 to the maximum extent practical consistent with the mission.

10.1.2 Dissemination of intelligence under this provision is authorized only if: (a) an authority designated by the military commander or civilian official determines that adherence to this DCID reasonably is expected to preclude timely dissemination to protect life or mission; (b) disseminations are for limited duration and narrowly limited to persons or entities that need the information within 72 hours to satisfy an imminent emergency need; and (c) there is insufficient time to obtain approval through normal intelligence disclosure channels.

10.1.3 The disclosing authority will report the dissemination through normal disclosure channels within 24 hours of the dissemination, or at the earliest opportunity thereafter as the emergency permits. For purposes of this provision, planning for contingency activities or operations not expected to occur within 72 hours does not constitute "imminent" need that warrants exercise of the emergency waiver to bypass the requirements of this DCID.

10.1.4 Military commanders and/or responsible civilian officials will ensure that written guidelines for emergency dissemination contain provisions for safeguarding

disseminated intelligence and notifying producers of disclosures of information necessary to meet mission requirements.

10.1.5 The NCA, and/or major commands or responsible civilian officials will immediately advise intelligence producers when the emergency situation ends.

## 11.0 Procedures Governing Use of Authorized Control Markings

11.1 Any recipient desiring to disseminate intelligence in a manner contrary to the control markings established by this Directive must obtain the advance permission of the agency that originated the intelligence. Such permission applies only to the specific purpose agreed to by the originator and does not automatically apply to all recipients. Producers of intelligence will ensure that prompt consideration is given to recipients' requests with particular attention to reviewing and editing, if necessary, sanitized or paraphrased versions to derive a text suitable for release subject to lesser or no control marking(s).

11.2 The control markings authorized above shall be shown on the title page, front cover, and other applicable pages of documents; incorporated in the text of electrical communications; shown on graphics; and associated (in full or abbreviated form) with data stored or processed in automated information systems. The control markings also shall be indicated by parenthetical use of the marking abbreviations at the beginning or end of the appropriate portions in accordance with E.O. 12958.

## 12.0 Obsolete Restrictions and Control Markings

12.1 The following control markings are obsolete and will not be used in accordance with the following guidelines:

12.1.1 WNINTEL and NOCONTRACT. The control markings, Warning Notice - Intelligence Sources or Methods Involved (WNINTEL), and NOT RELEASABLE TO CONTRACTORS/CONSULTANTS (abbreviated NOCONTRACT or NC) were rendered obsolete effective 12 April 1995. No permission of the originator is required to release, in accordance with this Directive, material marked WNINTEL. Holders of documents prior to 12 April 1995 bearing the NOCONTRACT marking should apply the policies and procedures contained in Section 6.1 for possible release of such documents.

12.1.2 Remarking of material bearing the WNINTEL, or NOCONTRACT, control marking is not required; however, holders of material bearing these markings may line through or otherwise remove the marking(s) from documents or other material.

12.1.3 Other obsolete markings include: WARNING NOTICE INTELLIGENCE SOURCES OR METHODS INVOLVED, WARNING NOTICE SENSITIVE SOURCES AND METHODS INVOLVED, WARNING NOTICE INTELLIGENCE SOURCES AND METHODS INVOLVED, WARNING NOTICE SENSITIVE INTELLIGENCE SOURCES AND METHODS INVOLVED, CONTROLLED DISSEM, NSC PARTICIPATING AGENCIES ONLY, INTEL COMPONENTS ONLY, LIMITED, CONTINUED CONTROL, NO DISSEM ABROAD, BACKGROUND USE ONLY, USIB ONLY, NFIB ONLY.

12.2 Questions with respect to current applications of all control markings authorized by earlier Directives on the dissemination and control of intelligence and used on documents issued prior to the effective date of this Directive should be referred to the agency or department originating the intelligence so marked.

### 13.0 Reporting Unauthorized Disclosures

13.1 Violations of the foregoing restrictions and control markings that result in unauthorized disclosure by one agency of the intelligence of another shall be reported to the Director of Central Intelligence through appropriate Intelligence Community channels.

### 14.0 Responsibilities of SOICs

14.1 SOICs shall be responsible for the implementation of internal controls and shall conduct training to ensure that the dissemination and release policies contained in this Directive and the limitations on the use of control markings are followed. SOICs shall assure that agency personnel are accountable for the proper marking of classified information under this Directive and Section 5.6 of EO 12958.

14.2 SOICs shall establish challenge procedures by which consumers may register complaints about the misuse of control markings or the lack of use of tear line reporting or portion marking. Information concerning such challenges shall be provided to the Security Policy Board staff upon request or for the annual review.

### 15.0 Annual Report on the Use of Control Markings

15.1 The Security Policy Board staff shall report to the DCI and Deputy Secretary of Defense on Intelligence Community compliance with this Directive, including the need for further policies in this area. The report will include an in-depth evaluation of the use of control markings in intelligence reporting/production, including consumer evaluations and producer perspectives on implementation of the Directive. The report shall also include information and statistics on challenges formally lodged under section 1.9 of Executive Order 12958 within and among intelligence agencies on the

use of control markings, including their adjudication and the number of times the authority in Section 10 was used and the documents provided. In order to inform the Security Policy Board staff of substantive detail in these areas for purposes of this review, Intelligence Community elements shall respond to requests for information from the Security Policy Board staff. Intelligence Community elements may build this program into their Self-Inspection programs under E.O. 12958. The Security Policy Board staff shall also obtain pertinent information on this subject from intelligence consumers as required.

15.2 The report required by this Section shall be conducted annually, unless otherwise directed by the DCI. The Staff Director, Security Policy Board shall establish the schedule for the report.

#### 16.0 Interpretation

16.1 Questions concerning the implementation of this policy and these procedures shall be referred to the Community Management Staff.

[signed]  
Director of Central Intelligence

30 June 1998  
Date

---

***[one page Classified Supplement DELETED]***

---

*[Footnotes]*

1. This Directive supersedes DCID 1/7, dated 12 April 1995.
2. Recipients will apprise originating agencies as to which components comprise the headquarters element and identify subordinate elements that may be included as direct recipients of intelligence information.
3. This provision is a requirement of the Trade Secrets Act, as amended (18 U.S.C 1905). The consent of the originator is required to permit release of material marked CAUTION - PROPRIETARY INFORMATION INVOLVED, PROPIN or PR to other than federal government employees.
4. For the purposes of implementing this portion of the DCID, "emergency situation" is defined as one of the following:
  - a) declared Joint Chiefs of Staff (JCS) alert condition of defense emergency, air defense emergency or DEFCON 3;
  - b) hostile action(s) being initiated against the United States or combined U.S./coalition/friendly forces;
  - c) U.S. persons or facilities being immediately threatened by hostile forces;
  - d) U.S. or combined U.S./coalition/friendly forces planning for or being deployed to protect or rescue U.S. persons, or U.S. /coalition/friendly forces;
  - e) U.S. civilian operations in response to U.S. or international disasters/catastrophes of sufficient severity to warrant Presidential declared disaster assistance/relief.

---

Original Classification: CONFIDENTIAL/NOFORN/X1

Approved for Release: DEC 2001

MORI DocID: 638921

Source: Courtesy of Jeffrey Richelson