



---

OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE  
INTELLIGENCE COMMUNITY POLICY MEMORANDUM  
NUMBER 2006-700-9

---

**SUBJECT:** (U) DIRECTOR OF NATIONAL INTELLIGENCE'S ACCEPTANCE OF COMMONWEALTH PARTNERS' ACCREDITATION APPROVALS FOR SOVEREIGN INFORMATION SYSTEMS PROCESSING US NATIONAL INTELLIGENCE INFORMATION

**A. AUTHORITY:** The National Security Act of 1947, as amended; the Intelligence Reform and Terrorism Prevention Act of 2004; Executive Order (EO) 12333, as amended, United States Intelligence Activities; EO 13355, Strengthened Management of the Intelligence Community; and other applicable provisions of law.

**B. PURPOSE:** This Intelligence Community (IC) Policy Memorandum (ICPM) updates Director of Central Intelligence Directive 6/3, Appendix E, Access by Foreign Nationals to Systems Processing Intelligence Information, with revised Director of National Intelligence (DNI) acceptance of Commonwealth Partners' accreditation approvals for sovereign information systems processing US national intelligence information.

**C. APPLICABILITY:** This ICPM applies to the IC, as defined by the National Security Act of 1947, as amended, and other departments or agencies that may be designated by the President, or designated jointly by the DNI and the head of the department or agency concerned, as an element of the IC.

**D. POLICY:** Effective immediately, the DNI will accept the accreditation approvals granted by the Principal Accrediting Authorities (PAAs) of US Commonwealth Partners, Australia, Canada, and the United Kingdom, for their respective sovereign information systems (ISs) that store, process, and/or communicate national intelligence information provided by the US government (USG).

1. This change is contingent upon the understanding that the Commonwealth PAAs shall:
  - a. Protect US national intelligence information commensurate with DNI policies.
  - b. Ensure that US national intelligence information is not further disseminated to other nations without US approval.

c. Certify and accredit such systems in accordance with their respective applicable national policies and guidelines.

d. Advise the Associate DNI/Chief Information Officer (ADNI/CIO) in writing of any further delegation of accreditation authority within their organizations.

e. Not approve connections of sovereign ISs that process US national intelligence information to other security domains without the written agreement of the ADNI/CIO.

f. Provide the DNI Special Security Center (SSC) with a yearly inventory of their respective sovereign ISs accredited under this agreement using reporting procedures and criteria provided by the SSC. This inventory shall include the name, number, or other unique IS identifier, owning entity, approved classification level and compartmentation of US information processed, accreditation approval and expiration dates, identification of any exceptions and mitigation plans, and PAA.

g. Promptly notify the SSC of any suspected or actual unauthorized disclosure of US intelligence information, provide sufficient detail to enable a preliminary damage assessment, initiate investigation of all circumstances of the incident, and cooperate in any resulting damage assessment.

2. (U) Definition

a. (U) The term *Commonwealth Partners* refers to Australia, Canada, and the United Kingdom for purposes of this document.

b. [REDACTED]

c. (U) An *information system* is any telecommunications and/or computer-related equipment or interconnected system or subsystems of equipment used in the acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of voice and/or data (digital or analog). The components of an IS typically include an operating system, applications, and services that are implemented in a combination of hardware, software, and firmware.

d. (U) The terms *national intelligence* and *intelligence related to national security* refer to all intelligence, regardless of the source from which derived and including information gathered within or outside the United States, as determined to be consistent with any guidance issued by the President, that pertains to more than one USG agency; that involves threats to the United States, its people, property, or interests; the development, proliferation, or use of weapons of mass destruction; or any other matter bearing on US national or homeland security.

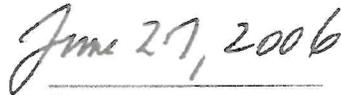
e. (U) A *security domain* is a discrete IS identified by its authorized classification level and/or releasability to foreign nationals, or a collection of IS with a common authorized classification level and/or releasability constraint.

f. (U) A *sovereign information system* is an IS (as defined) that is wholly owned, operated, used, and maintained by the Commonwealth country.

**E. EFFECTIVE DATE:** This ICPM becomes effective on the date of signature and the contents will be incorporated into an IC directive.



\_\_\_\_\_  
Director of National Intelligence



\_\_\_\_\_  
Date