# INTELLIGENCE COMMUNITY DIRECTIVE

# NUMBER 503

## INTELLIGENCE COMMUNITY
## INFORMATION TECHNOLOGY SYSTEMS SECURITY
## RISK MANAGEMENT, CERTIFICATION AND ACCREDITATION

(EFFECTIVE 15 SEPTEMBER 2008)

**A. AUTHORITY:** The National Security Act of 1947, as amended; The Federal Information Security Management Act of 2002, as amended; Executive Order (EO) 12333, as amended; EO 13231; EO 12958, as amended; and other applicable provisions of law.

**B. PURPOSE:** This Intelligence Community Directive (ICD) establishes Intelligence Community (IC) policy for information technology systems security risk management, certification and accreditation.

1. This policy implements strategic goals agreed upon in January 2007 by the IC Chief Information Officer (CIO), the Chief Information Officers of the Department of Defense (DoD), the Office of Management and Budget, and the National Institute of Standards and Technology (NIST). This ICD focuses on a more holistic and strategic process for the risk management of information technology systems, and on processes and procedures designed to develop trust across the intelligence community information technology enterprise through the use of common standards and reciprocally accepted certification and accreditation decisions.

2. This ICD rescinds and replaces the Director of Central Intelligence Directive (DCID) 6/3 Policy, Protecting Sensitive Compartmented Information within Information Systems, and the associated DCID 6/3 Manual having the same title. It also rescinds the DCID 6/5 Implementation Manual for the Protection of Certain non-Sensitive Compartmented Information (SCI) Sources and Methods Information (SAMI). Appendix E in the DCID 6/3 Manual, Access by Foreign Nationals to Systems Processing Intelligence, shall remain in effect until subsequent issuances supersede it.

**C. APPLICABILITY:** This ICD 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 Director of National Intelligence and the head of the department or agency concerned, as an element of the IC.

## D. POLICY

### 1. Risk Management

a. The principal goal of an IC element's information technology risk management process shall be to protect the element's ability to perform its mission, not just its information assets. Therefore, IC elements shall consider risk management an essential management function, and shall ensure that it is tightly woven into the system development life cycle.

b. Because risk cannot be eliminated entirely, the risk management process must allow decision makers to consider the operational and economic costs of protective measures weighed against requirements for mission accomplishment. For example, a very high level of security may reduce risk to a very low level, but can be extremely expensive, and may unacceptably impede essential operations.

(1) In determining the level of acceptable risk associated with the operation of an information technology system at a particular level of security, IC elements shall give appropriate weight to the often competing equities of mission and security requirements, budget consequences, operational performance efficiencies, schedule requirements, counterintelligence concerns, civil liberties and privacy protection, and other relevant policy requirements.

(2) Elements of the IC shall weigh the potential costs of protective measures against security benefits gained, ensuring that security measures adopted and applied allow mission capabilities at acceptable risk levels.

(3) Elements of the IC shall consider information sharing and collaboration across the IC and with appropriate foreign partners as essential mission capabilities.

c. Elements of the IC shall determine the level of security required for an information system by considering the sensitivity of the information contained within the system, and by evaluating the system's ability to permit information sharing and collaboration across the IC.

d. Many IC information systems are interconnected. Therefore, the risk accepted by one element is effectively accepted by all, just as security limitations imposed by one are effectively imposed upon all. To promote interoperability and efficiency across the IC information technology enterprise, and to provide a sound basis for trust and reciprocal acceptance of individual element certification and accreditation across the enterprise, IC elements shall apply common standards and follow a common process to manage risk for their systems.

e. Elements of the IC shall apply standards for information technology risk management established, published, issued, and promulgated by the IC CIO. Information technology risk management standards published, issued, and promulgated for the IC by the IC CIO may include standards, policies and guidelines approved by either or both NIST and the Committee on National Security Systems (CNSS).

2. **Accreditation**

a. Accreditation decisions are official management decisions that explicitly accept a defined level of risk associated with the operation of an information technology system at a particular level of security in a specific environment on behalf of an IC element.

b. By accrediting an information system, an IC element approves it for operation at a particular level of security in a particular environment, and thus establishes the level of risk associated with operating the system and the associated implications for operations, assets, or individuals.

c. In determining the level of acceptable risk associated with the operation of an information technology system, IC elements shall make decisions on accreditation in accordance with the policy for risk management described in this Directive and in any standards that may be subsequently issued pursuant to the authorities granted herein.

d. Accreditation by IC elements shall ensure that risk is mitigated to the extent possible, commensurate with the sensitivity of the information in a system. Elements shall ensure that accreditation of their systems permits IC-wide collaboration and information sharing sufficient to ensure both element and IC-wide mission accomplishment. In accrediting any system over which it has accreditation authority as described below, an element shall accept only the minimum degree of risk required to ensure that the information system effectively supports mission accomplishment while appropriately protecting the information in the system.

e. The head of each IC element may designate one or more Authorizing Officials to make accreditation decisions on behalf of the element head. The element head shall retain ultimate responsibility for all accreditation and associated risk management decisions made on his or her behalf.

(1) An Authorizing Official shall be accountable to the element head for the accreditation and associated risk management decision, for which the element head is ultimately responsible and accountable.

(2) An Authorizing Official has inherent U.S. Government authority and, as such, must be a government employee.

(3) An Authorizing Official shall have a broad and strategic understanding of the IC and of his or her particular IC element and its place and role in the overall IC. An Authorizing Official shall use this knowledge to assign appropriate weight to the often competing equities of mission and security requirements, budget consequences, operational performance efficiencies, schedule requirements, counterintelligence concerns, information sharing, civil liberties and privacy protection, and other relevant policy requirements. Then, in light of these factors, the Authorizing Official will determine the level of risk deemed acceptable for an accredited system.

(4) An Authorizing Official should normally be the agency or element CIO. For IC elements without a CIO, an Authorizing Official shall be an executive of sufficient seniority to execute the decision-making and approval responsibilities described above on behalf of the element.

(5) An IC element Authorizing Official shall accredit or reaccredit systems the element funds, operates, or manages, as well as any operated by the element as an executive agent on behalf of the IC enterprise.

(6) An Authorizing Official's accreditation decision shall articulate the supporting rationale for the decision, provide an explanation of any terms and conditions for the authorization, and explain any limitations or restrictions imposed on the operation of the system and the reasons for those limitations or restrictions. An Authorizing Official shall state, in the accreditation decision documentation, whether the system is accredited, accredited with conditions, or not accredited.

f. An Authorizing Official may appoint one or more Delegated Authorizing Officials to expedite accreditation approval of designated systems, and provide mission support.

(1) A Delegated Authorizing Official has inherent U.S. Government authority and, as such, must be a government employee.

(2) Like an Authorizing Official, a Delegated Authorizing Official shall have a broad and strategic understanding of the IC and of his or her particular IC element and its place and role in the overall IC. A Delegated Authorizing Official shall use this knowledge to assign appropriate weight to the often competing equities of mission and security requirements, budget consequences, operational performance efficiencies, schedule requirements, counterintelligence concerns, civil liberty and privacy protection, and other relevant policy requirements, and then in light of these factors, to determine the level of risk deemed acceptable for an accredited system.

g. In determining which particular information systems may be accredited by a Delegated Authorizing Official, an Authorizing Official shall consider the potential impact on organizations or individuals should there be a breach of security of a particular system such that a loss of information confidentiality, integrity or availability results.

(1) Confidentiality means the preservation of authorized restrictions on information access and disclosure, including means for protecting personal privacy, proprietary information, and classified information. A loss of confidentiality is the unauthorized disclosure of information.

(2) Integrity means the prevention of improper modification or destruction of information and includes ensuring information non-repudiation and authenticity. A loss of integrity is the unauthorized modification or destruction of information.

(3) Availability means ensuring timely and reliable access to and use of information. A loss of availability is the disruption of access to or use of information in an information system.

h. A Delegated Authorizing Official shall only accredit an information system if the Authorizing Official determines that a breach of security of that information system would result in no more than a low to moderate potential impact on organizations or individuals. In no case shall a Delegated Authorizing Official make an accreditation decision for a system when an Authorizing Official deems a breach of security of that information system would result in a high potential impact on organizations or individuals.

(1) The potential impact is low if the loss of confidentiality, integrity or availability could be expected to have a limited adverse impact on organizational operations, organizational assets, or individuals. Examples of a limited adverse impact are losses of confidentiality, integrity or availability that might cause any of the following:

(a) a degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is noticeably reduced

(b) minor damage to organizational assets;

(c) minor financial loss; or

(d) minor harm to individuals.

(2) The potential impact is moderate if the loss of confidentiality, integrity or availability could be expected to have a serious adverse impact effect on organizational operations, organizational assets, or individuals. Examples of a serious adverse impact are losses of confidentiality, integrity, or availability that might cause any of the following:

a) degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but effectiveness of the functions is reduced significantly;

b) significant damage to organizational assets; or

c) significant harm to individuals that does not involve loss of life or serious life threatening injuries.

(3) The potential impact is high if the loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse impact on organizational operations, organizational assets, or individuals. Examples of a severe or catastrophic adverse impact are losses of confidentiality, integrity, or availability that might cause any of the following:

a) degradation in mission capability to an extent and duration that the organization is not able to perform one or more of its primary functions;

b) major damage to organizational assets;

c) major financial loss; or

d) significant harm to individuals involving loss of life or serious life threatening injuries.

i. Elements of the IC shall provide appropriate accreditation documentation to IC and DoD elements, if requested, to support reciprocity and re-use.

j. Elements of the IC shall establish a formally-defined stake-holder appeal process to resolve any conflicts resulting from Authorizing Official or Delegated Authorizing Official decisions. Such conflicts might include disagreements on the competing equities of mission and security requirements, budget consequences, operational performance efficiencies, schedule requirements, counterintelligence concerns, civil liberty and privacy protection, and other relevant policy requirements.

k. Elements of the IC shall apply standards for accreditation processes and decisions, including impact levels that may be determined in addition to those discussed above, as may be published, issued, and promulgated by the IC CIO in the future. Information technology accreditation process and decision standards published, issued, and promulgated for the IC by the IC CIO may include standards, policies and guidelines approved by either or both NIST and CNSS.

3. **Certification**

a. A security certification is the required comprehensive assessment of the management, operational, and technical security controls in an information technology system, or for a particular item of information technology, made in support of accreditation.

(1) An information technology system is a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination or disposition of information.

(2) An item of information technology is any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information. The term "information technology" includes computers, ancillary equipment, software, firmware and similar procedures, services (including support services), and related resources.

b. A security certification shall provide the essential information technology systems security analysis needed to make a credible, risk-based decision on whether to authorize operation of the information system or of an item of information technology (that is, upon which to make the accreditation decision).

c. A security certification shall serve as the information technology systems security portion of the factors, equities and concerns upon which an Authorizing Official or Delegated Authorizing Official shall base an accreditation decision appropriately accepting risk in accordance with the policies set forth by this Directive.

d. An Authorizing Official shall appoint a Certification Agent to act on his or her behalf to conduct a security certification. A Certification Agent may not also be an Authorizing Official or a Designated Authorizing Official.

e. The Authorizing Official or Designated Authorizing Official shall use the results of the security certification as input to the accreditation decision.

f. A Certification Agent may not approve an accreditation on behalf of an Authorizing Official or a Designated Authorizing Official.

g. Elements of the IC shall apply standards for security certification assessment, testing, process and reporting published, issued and promulgated by the IC CIO. Information technology certification standards published, issued and promulgated for the IC by the IC CIO may include standards, policies and guidelines approved by either or both NIST and CNSS.

4. **Reciprocity**

a. Elements of the IC shall make appropriate accreditation documentation available to other IC elements, and to the non-IC parts of the DoD generally, its Military Departments, Combatant Commands and Defense Agencies, and also to non-IC agencies of the Federal Government.

b. Authorizing Officials of IC elements shall make appropriate certification documentation of an information technology system or other item of information technology available to other IC elements, to the non-IC parts of the DoD generally, its Military Departments, Combatant Commands and Defense Agencies, and to other non-IC agencies of the Federal Government.

c. An IC element shall accept the certification of a system or other item of information technology by another IC element without requiring or requesting any additional validation or verification testing of the system or item of information technology.

(1) Elements of the IC shall test only the configuration differences introduced by using the system or item of information technology in a new or different environment.

(2) Authorizing Officials and Delegated Authorizing Officials of IC elements shall consider the original IC element certification when making the accreditation decision for placing a system or item of information technology of another IC element into operation as a new or additional part of any system for which the Authorizing Official or Delegated Authorizing Official exercises accreditation authority.

d. Elements of the IC shall accept a certification of an information system or of an item of information technology of any non-IC agency of the Federal Government, or of a state, tribal or non-governmental agency, organization, or contractor, if that certification is based on standards compatible with those established for the IC in accordance with this Directive (such as, for example, either or both NIST and CNSS standards issued for the IC by the IC CIO pursuant to the authority granted in this Directive), without requiring or requesting any additional validation or verification testing of the system or item of information technology.

(1) Elements of the IC may test only the configuration differences introduced by using the system or the item in a new environment.

(2) IC element Authorizing Officials and Delegated Authorizing Officials shall consider the original agency, state, tribal or non-governmental agency, organization, or contractor certification when making the accreditation decision for placing a system or item of information technology of a non-IC system into operation as part of a new or additional system for which the Authorizing Official or Delegated Authorizing Official exercises accreditation authority, if that certification is based on standards compatible with those established for the IC in accordance with this Directive (such as, for example, either or both NIST and CNSS standards issued for the IC by the IC CIO pursuant to the authority granted in this Directive).

e. All IC elements shall accept accreditations granted by the Commonwealth/5-Eyes Partners (Australia, Canada, New Zealand, United Kingdom) for their respective sovereign information technology systems or items of information technology that store, process, and/or communicate national intelligence information provided by the U.S. Government.

5. **Interconnection**

a. Elements of the IC shall permit interconnections of accredited information technology systems with the accredited systems of other IC elements in accordance with standards for system interconnection published, issued and promulgated by the IC ClO. Information technology system interconnection standards published, issued, and promulgated for the lC by the IC CIO may include standards, policies and guidelines approved by either or both NIST and CNSS.

b. Elements of the IC may permit interconnection of accredited information technology systems with the information technology systems of U.S. Government, state, tribal and non-governmental agencies, organizations, entities, contractors and elements outside of the IC in accordance with standards for system interconnection published, issued, and promulgated by the IC CIO. Information technology system interconnection standards published, issued, and promulgated for the IC by the IC CIO may include standards, policies and guidelines approved by either or both NIST and CNSS.

c. Standards for interconnection established in accordance with paragraph 5.a. and b. above may require the use of an interconnection security agreement. The interconnection security agreement is a security document that defines the technical and security requirements for establishing, operating and maintaining the connection. The IC CIO shall identify the standards required in an interconnection security agreement, if required by applicable standards.

d. The IC CIO shall identify and define the guidelines and standards for connecting IC systems to systems operated by Commonwealth Partners, and shall update guidelines and standards at intervals appropriate for that purpose.

e. The IC CIO shall identify and define the guidelines and standards for connecting IC systems to systems operated by foreign nationals other than Commonwealth Partners, and shall update guidelines and standards, at intervals appropriate for that purpose.

6. **Governance and Dispute Resolution**

a. The IC CIO shall monitor IC element compliance with this Directive to ensure that elements appropriately certify systems, and accredit systems within acceptable levels of community risk.

b. In the event an IC element finds that the reciprocal acceptance of an interconnection decision, a risk management decision or a certification of another IC element creates a degree of risk or imposes a level of security that results in unacceptable or incompatible consequences either for that element, or for the IC as a whole, the concerned element Authorizing Official shall refer the matter to the IC CIO.

(1) The IC CIO shall mediate the matter and, if unresolved, make recommendations to the IC element heads.

(2) In making this recommendation, the IC CIO shall give appropriate weight to the often competing equities of mission and security requirements, budget consequences, operational performance efficiencies, schedule requirements, counterintelligence concerns, information

sharing, civil liberties and privacy protection, and other relevant policy requirements, and balance risk in accordance with this Directive.

**E. EFFECTIVE DATE:** This ICD becomes effective on the date of signature. IC elements may continue to operate systems and items of information technology currently certified and accredited under pre-existing policies, guidelines and standards; any certification, recertification, accreditation, or reaccreditation of existing and currently certified and accredited systems or items of information technology undertaken after the date of signature must, however, be accomplished in accordance with the policies set forth in this Directive. Any information systems or items of information technology placed into service after the date of signature shall be certified and accredited in accordance with the policies set forth in this Directive.

J M McConnell

Director of National Intelligence

15 SEP 08

Date

# APPENDIX A – ACRONYMS

## ICD 503 – INTELLIGENCE COMMUNITY INFORMATION TECHNOLOGY SYSTEMS SECURITY RISK MANAGEMENT, CERTIFICATION AND ACCREDITATION

| | |
|---|---|
| CIO | Chief Information Officer |
| CNSS | Committee on National Security Systems |
| DCID | Director of Central Intelligence Directive |
| DoD | Department of Defense |
| EO | Executive Order |
| IC | Intelligence Community |
| ICD | Intelligence Community Directive |
| NIST | National Institute of Standards and Technology |
| SCI | Sensitive Compartmented Information |