

Intelligence Community Information Environment Risk Management

A. AUTHORITY: The National Security Act of 1947, as amended; The Federal Information Security Modernization Act (FISMA) of 2002, as amended; Intelligence Reform and Terrorism Prevention Act of 2004; Privacy Act of 1974; Executive Order 12333, as amended; and other applicable provisions of law.

B. PURPOSE: This Intelligence Community Directive (ICD) establishes Intelligence Community (IC) policy governing and assigning responsibilities for the management of risk for the IC Information Environment (IC IE). This ICD supersedes ICD 503, *Intelligence Community Information Technology Systems Security Risk Management*, 21 July 2015.

C. APPLICABILITY

1. This Directive applies to the IC, as defined by the National Security Act of 1947, as amended, and to such other elements of any department or agency as may be designated by the President, or designated jointly by the Director of National Intelligence (DNI) and the head of the department or agency concerned, as an element of the IC.

2. This Directive applies to the IC IE which, as defined in ICD 121, *Managing the Intelligence Community Information Environment*, includes the individuals, organizations, and information technology (IT) capabilities that collect, process, or share Sensitive Compartmented Information, or that, regardless of classification, are operated by the IC and are in whole or in majority funded by the National Intelligence Program.

D. POLICY

1. *IC IE Risk Management*

a. The principal goal of an IC element's IT risk management process shall be to protect the element's ability to perform its mission. Therefore, IC elements shall take a structured approach to oversee and manage risk within an interconnected IC IE where the risk accepted by one IC element is effectively accepted by all IC elements.

b. The IC IE shall operate in accordance with a Risk Management Framework (RMF) that promotes security, privacy, interoperability, and efficiency. Implementing such a framework will establish a sound basis for trust and reciprocal acceptance of security and privacy assessments and authorization decisions across the IC. Reciprocal acceptance of security and privacy assessments and authorization decisions does not confer data reciprocity.



INTELLIGENCE
COMMUNITY
DIRECTIVE

503

(1) The IC Chief Information Officer (IC CIO) shall establish and ensure the IC's RMF aligns with current best practices, to the maximum extent practical, and that security standards support and facilitate reciprocity, interconnection, information sharing, and dispute resolution in order to balance security and privacy risks with protecting mission performance and mission requirements.

(2) To manage risk for the IC IE, IC elements shall implement security and privacy standards in accordance with IC policy, and other guidance issued by the IC CIO and the Civil Liberties Protection Officer (CLPO), respectively. While separate and distinct disciplines, security and privacy are inextricably intertwined in the IC IE. To effectively identify and manage risk, and facilitate compliance with applicable requirements, a consistent IC approach to implementing the RMF is required, especially where security and privacy objectives overlap.

(3) IC elements shall implement Zero Trust security principles, consistent with National Security Memorandum-8, *Improving the Cybersecurity of National Security, Department of Defense, and Intelligence Community Systems*, which acknowledges that threats exist both inside and outside traditional network boundaries. The implementation of Zero Trust security principles eliminates implicit trust and instead requires continuous verification based on real-time information to determine access and other system responses.

(4) IC elements shall implement robust Information Security Continuous Monitoring (ISCM), to maintain ongoing awareness of information security, vulnerabilities, and threats, in support of organizational risk management decisions, in accordance with ICD 502, *Integrated Defense of the Intelligence Community Information Environment*.

(5) IC elements shall collaborate with one another, to the extent necessary, in the implementation of the RMF.

(6) IC elements shall consider information sharing and collaboration across the IC and with appropriate foreign partners as essential mission capabilities when implementing the RMF.

c. The IC CIO shall serve as:

(1) The Accountable Official for the implementation of this policy, and oversee management of security risk for the IC IE, in coordination with the CLPO and the IC Chief Data Officer (IC CDO); and

(2) The DNI's designee for performing all applicable FISMA responsibilities including:

(a) Developing and overseeing the implementation of principles, standards, and guidelines for information security; and

(b) Requiring IC elements to identify and provide information security protections commensurate with the risk and magnitude of harm resulting from the unauthorized access, use, disclosure, disruption, modification, or destruction of information or information systems.

d. The IC CIO shall designate a Chief Information Security Officer for the IC (IC CISO). The IC CISO shall serve as the Senior Agency Information Security Officer (SAISO) of the IC and be responsible for the implementation of the overall IC information systems security

program as well as monitoring overall IC compliance with information systems security policies, standards, and procedures.

e. The CLPO shall oversee management of privacy risk for the IC IE, in accordance with ICD 107, *Civil Liberties, Privacy, and Transparency*, and ICD 121, in coordination with the IC CIO and the IC CDO, and ensure the IC's RMF aligns with current best practices, to the maximum extent practical.

f. To identify and implement the most robust defensive measures possible, IC IE risk management activities shall be coordinated by the IC CIO, to the maximum extent practical, with stakeholders performing related or integrated activities throughout the IC, to include the:

(1) Supply chain risk management activities of the National Counterintelligence and Security Center (NCSC); and

(2) Cyber threat intelligence activities of the Cyber Executive.

g. Supply chain risk shall be considered an integral element of security risk and managed in accordance with ICD 731, *Supply Chain Risk Management*.

2. *Authorization Decisions*

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

b. Authorization decisions are made by an Authorizing Official (AO). The head of each IC element may designate one or more AOs to make authorization decisions on their behalf.

(1) An AO shall be accountable to the IC element head for the authorization and associated risk management decision, for which the IC element head is ultimately responsible and accountable.

(2) AOs have inherent U.S. Government authority and, as such, must be a government employee.

(3) An AO shall have a broad and strategic understanding of the IC and of their particular IC element and its place and role in the overall IC. An AO 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 AO will determine the level of risk deemed acceptable for an authorized system.

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

(5) The IC CIO is the Authorizing Official, and shall appoint a Security Assessor, for IC IT Services of Common Concern (SoCC) as described in ICD 121, and provides the framework for security assessments and authorization decisions for IC IT SoCC in consultation

with IC IT Service Providers and affected IC elements. The IC CIO may designate an IC IT Service Provider as the Authorizing Official, who shall appoint a Security Assessor, on a case-by-case basis consistent with this Directive and ICD 122, *Services of Common Concern*.

(6) An IC element AO shall, consistent with the designation in Section D.2.b.(5) above, make authorization decisions for systems the IC element funds, operates, or manages, as well as any operated by the IC element as an IC IT SoCC.

(7) An AO's authorization 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. An AO shall state, in the authorization decision documentation, whether the system is authorized for operation, authorized for operation with conditions, or not authorized for operation.

c. An AO may appoint one or more Delegated Authorizing Officials (DAO) to expedite authorization decisions for designated systems, and provide mission support.

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

(2) Like an AO, a DAO shall have a broad and strategic understanding of the IC and of their particular IC element and its place and role in the overall IC. A DAO 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. Then in light of these factors, the DAO will determine the level of risk deemed acceptable for an authorized system.

(3) In determining which particular information systems may be authorized by a DAO, an AO shall consider the potential impact on organizations or individuals should there be a privacy or security breach of a particular system such that a loss of information confidentiality, integrity, or availability results.

(4) A DAO shall only authorize an information system if the AO determines that a security or privacy breach 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 DAO make an authorization decision for a system when an AO deems a security or privacy breach of that information system would result in a high potential impact on organizations or individuals.

(a) A 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.

(b) A potential impact is moderate if the loss of confidentiality, integrity, or availability could be expected to have a serious adverse impact on organizational operations, organizational assets, or individuals.

(c) A 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.

d. An AO shall evaluate and approve each information system within their purview on each security fabric (e.g., Top Secret, Secret, or Unclassified) and within each environment to establish the level of risk associated with operating the system and the associated implications for organizational operations, organizational assets, or individuals.

e. IC elements shall make authorization decisions and subsequent risk level decisions for the operation of an information system in accordance with applicable provisions of law and policy.

f. Authorization decisions by IC elements shall ensure that risk is considered commensurate with the sensitivity of the information processed by the system, and appropriate mitigations are implemented to the fullest extent possible. IC elements 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 to the fullest extent possible.

g. Authorization decisions shall be based on security and privacy assessments, mitigation efforts, and the potential impact on organizations and individuals should there be a security or privacy breach of a particular system.

h. IC elements shall apply standards for authorization processes and decisions, including impact levels that may be determined in addition to those discussed above, as issued by the IC CIO.

i. The IC element's AO shall notify the IC CIO when they accept an item of IT for an IT system with high or critical residual risk when a security or privacy breach of that system would result in a high potential impact. For the purposes of this policy:

(1) An IT 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 IT 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.

3. Security and Privacy Assessment

a. A security and privacy assessment is the required comprehensive assessment of the management, operations, and technical security and privacy controls for an information system, or for a particular item of IT, made in support of authorization decisions. When producing a security and privacy assessment, IC elements shall apply IC standards issued by the IC CIO for security assessments, testing, processes, and reporting. IC elements shall apply IC standards issued by the CLPO for privacy assessments, testing, processes, and reporting.

b. A security and privacy assessment shall provide the essential information systems analysis needed to make a credible, risk-based decision on whether to authorize operation of the IT system or of an item of IT.

c. A security and privacy assessment shall evaluate the IT, systems security and privacy risk mitigation factors, and IC equities and concerns upon which an AO or DAO shall base an authorization decision.

d. An Authorizing Official shall appoint a Security Assessor to act on their behalf to conduct a security and privacy assessment. A Security Assessor may not also be an AO or a DAO and may not approve an authorization decision on behalf of an AO or DAO.

e. Community Shared Resources that generate user attributable audit records shall do so in accordance with IC policy. Security Assessors shall collaborate with the IC elements' counterintelligence insider threat program offices to validate that the records' contents satisfy security investigative requirements. For the purposes of this policy, a Community Shared Resource is an information resource or system that a person or non-person entity existing outside the resource-owning element's organizational network boundary can access.

4. *Reciprocity*

a. IC elements shall share authorization decision documentation, as well as security and privacy assessment documentation, with other IC elements, the non-IC elements of Department of Defense (DoD), and non-IC elements of the federal government, as appropriate and consistent with applicable provisions of law and policy. To the maximum extent possible, IC elements shall enter into reciprocal agreements for sharing such documentation. IC elements shall notify the IC CIO when authorization decision documentation is shared with non-IC elements of DoD and non-IC elements of the federal government.

b. IC elements shall, to the maximum extent practical, accept the security and privacy assessment of an information system, cloud service, or other item of IT by another IC element without requiring or requesting any additional validation or verification testing of the system, service, or item of IT from the IC element, unless deemed necessary by that IC element's AO. However, IC elements should test configuration differences introduced by the system, service, or the item in a new environment.

c. IC elements shall leverage, to the maximum extent possible, security and privacy assessments of an information system, cloud service, or an item of IT from any non-IC element of DoD, non-IC element of the federal government, or of a state, local, tribal or non-governmental agency, organization, or contractor, if that assessment is based on standards consistent with those established for the IC, without requiring or requesting any additional validation or verification testing of the system, service, or item of IT, unless deemed necessary by that IC element's AO. However, IC elements should test configuration differences introduced by the system, service, or the item in a new environment.

d. All IC elements shall accept authorization decisions granted by Five Eyes partners for their respective sovereign information systems, services, or items of IT at equivalent classification levels that store, process, and/or communicate national intelligence information provided by the U.S. Government. IC elements shall, to the maximum extent possible, enter into reciprocal agreements for sharing authorization decision documentation as well as security and privacy assessment documentation with Five Eyes partners.

e. In the event that an IC element finds that sharing documentation, reciprocal acceptance of an interconnection decision, a risk management decision, an authorization decision, or a security or privacy assessment of another IC element, or other entity discussed in this section, creates a degree of risk or imposes a level of security that results in unacceptable or incompatible consequences either for that IC element or for the IC as a whole, the concerned IC element's AO shall refer the matter to the IC CIO.

(1) The IC CIO shall mediate the matter, as appropriate, and in consultation with the CLPO as appropriate and, if unresolved, make recommendations to the concerned IC element head.

(2) In making these recommendations, 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.

5. *Interconnection*

a. IC elements shall permit interconnection of authorized IT systems with the authorized systems of other IC elements, as well as DoD, federal, state, local, tribal, non-governmental, and foreign partners, in accordance with applicable standards for system interconnection established by the IC CIO.

b. Standards for interconnection established in accordance with this section 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, as needed.

c. The IC CIO shall develop the guidelines and standards for connecting IC systems to systems operated by domestic and foreign partners to facilitate secure and robust information sharing, consistent with applicable law, policy, and strategy.

E. ROLES AND RESPONSIBILITIES

1. The IC CIO shall:

- a. Serve as the Accountable Official for the implementation of this policy;
- b. Issue IC Standards, as necessary, to implement this Directive in accordance with IC Policy Guidance (ICPG) 101.2, *Intelligence Community Standards*;
- c. Develop and oversee a secure IC IE that meets mission needs and facilitates robust information sharing, both within the IC as well as with domestic and foreign partners, while maintaining privacy, in coordination with CLPO and IC CDO;
- d. Designate, in writing, a government official to serve as the IC CISO;
- e. Develop and implement:

- (1) A common set of security standards, processes, and procedures for the IC IE to manage security risk, in coordination and in alignment with the CLPO and IC CDO;
 - (2) Guidelines and standards for connecting IC systems to systems operated by domestic and foreign partners to facilitate secure and robust information sharing, consistent with applicable law, policy, and strategy; and
 - (3) Communicate and coordinate with CLPO, as necessary, when an IC element AO notifies IC CIO of accepting an item for an IT system that could result in a high potential impact if breached consistent with Section D.2.i.;
- f. Monitor, evaluate, and ensure:
- (1) Compliance with established IC IE policies, standards, guidelines, processes, and procedures across the IC; and
 - (2) The performance of all IC IE programs on the basis of applicable performance measurements and, in coordination with relevant IC element CIOs, advise the DNI regarding whether to continue, modify, or terminate programs.
- g. Adjudicate and mediate disputes between IC elements, in consultation with CLPO as appropriate, regarding the acceptance of risk and reciprocity as described in Section D.4.e.;
- h. Provide guidance and direction to all IC IE-related acquisition and procurement processes to ensure risk management integration and consistency with applicable provisions of law and policy, relevant standards, and strategic goals;
- i. Designate AOs for IC IT SoCCs, in coordination with the head of the designated IC element Service Provider, in accordance with Section D.2.b.(5);
- j. Oversee security assessments, to include the use of joint test teams for IC IT SoCCs, and review the security compliance, penetration testing results, and authorization activities for:
- (1) All IC IT SoCCs; and
 - (2) All IT systems destined for use by more than one IC element, such as, but not limited to components related to IC IT SoCCs, Community Shared Resources, and other IT systems identified with a security categorization of “high,” into which the DNI needs insight;
- k. Determine acceptable risk and suitability, in consultation with IC IT SoCC Providers and IC element AOs to ensure IC IT SoCCs have established an acceptable level of risk prior to becoming operational in the shared space; and
- l. Consistent with applicable provisions of law and policy, and Section D.1.f., coordinate with the NCSC and Cyber Executive.
2. The IC CISO shall:
- a. Implement the overall IC information systems security program;
 - b. Serve as SAISO for the IC;

- c. Monitor overall IC compliance with information systems security policies, standards, and procedures;
- d. Chair the IC Chief Information Security Officer Committee, or successor committee;
- e. As appropriate and consistent with applicable provisions of law and policy, coordinate on IT security risks with operational performance measures and vulnerability management activities in accordance with ICD 502;
- f. Develop and maintain central IC repositories of inheritable security and privacy controls and best practices; and
- g. Support the IC CIO in annual reporting to the DNI on the effectiveness of the IC's information system security program.

3. The CLPO shall:

- a. Oversee management of privacy risk for the IC IE, in accordance with ICD 107 and ICD 121, in coordination with the IC CIO and the IC CDO, and ensure the IC's RMF aligns with current best practices, to the maximum extent practical;
- b. Issue IC Standards, as necessary, pertaining to management of privacy risk in accordance with ICD 107 and ICPG 101.2; and
- c. Develop and implement a common set of privacy standards, processes, and procedures for the IC IE to manage privacy risk, in coordination and in alignment with IC CIO and IC CDO.

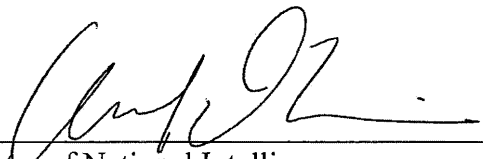
4. Heads of IC elements shall:

- a. Establish, manage, and maintain security and privacy risk management processes to ensure compliance with this Directive and applicable provisions of law and policy;
- b. Apply applicable security and privacy standards and controls to all mission, business, and enterprise IT under their purview;
- c. Designate, in writing, one or more AOs and DAOs, as appropriate, to make authorization decisions for IT systems on their behalf, while retaining ultimate responsibility for all authorization and associated risk management decisions;
- d. Implement robust ISCM to maintain ongoing awareness of information security, vulnerabilities, and threats to support organizational risk management decisions;
- e. Ensure the acquisition, design, development, integration, distribution, operation, maintenance, and retirement of systems under their purview integrate security and privacy risk management throughout the processes;
- f. Reciprocally share, accept, or leverage authorization decisions and security and privacy assessments, in accordance with Section D.4.;
- g. Consider information sharing and collaboration across the IC and with appropriate foreign partners as essential mission capabilities when implementing the RMF;

h. Establish interconnection security agreements as needed and permit interconnections of authorized information systems with the authorized systems of other IC elements, as well as DoD, federal, state, local, tribal, non-governmental, and foreign partners, in accordance with applicable standards for system interconnection established by the IC CIO; and

i. Actively lead or support interagency joint testing activities, as possible.

F. EFFECTIVE DATE: This Directive becomes effective on the date of signature. IC elements may continue to operate systems and items of IT currently assessed and authorized under pre-existing policies, guidelines and standards. Any assessment, reassessment, authorization, or reauthorization of existing assessed and authorized systems or items of IT 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 IT placed into service after the date of signature shall be assessed and authorized in accordance with the policies set forth in this Directive.



Director of National Intelligence

OCT 25 2024

Date