INTELLIGENCE COMMUNITY DIRECTIVE 121

Managing the Intelligence Community Information Environment

A. AUTHORITY: The National Security Act of 1947, as amended; Executive Order (EO) 12333, as amended, and other applicable provisions of law.

B. PURPOSE

1. This Intelligence Community (IC) Directive (ICD) establishes policy for an IC enterprise approach to managing the IC Information Environment (IC IE) in support of the IC mission through establishing roles and responsibilities, and it provides guidance on using a Service Provider model; information sharing and safeguarding; and information technology (IT) infrastructure and capabilities.

2. An IC enterprise approach for managing the IC IE will:

a. Advance intelligence integration and enable deeper analytic collaboration across IC elements through increased and accelerated communication, information sharing and safeguarding, transparency, and discovery of and access to information; and

b. Consolidate IT capabilities and infrastructure, and the acquisition and procurement thereof, resulting in increased efficiency and reduced duplication.

3. This ICD rescinds ES 00564, *Guiding Principles for Implementing and Operating in a Common Intelligence Community Information Technology Enterprise*, 19 September 2013, and ES 00124, *Leveraging the Intelligence Community Information Technology Enterprise*, 29 March 2013.

C. APPLICABILITY

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

2. This guidance applies to the IC IE which, consistent with ICD 502, *Integrated Defense of the IC IE*, includes the individuals, organizations, and 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 elements shall first use an IC enterprise approach, which accounts for all IC equities and enhances intelligence integration, for managing the IC IE before using an IC element-centric solution.

a. In instances where there is an IC IT Service of Common Concern (hereafter "IC IT SoCC") and an IC element asserts it has unique infrastructure or enterprise architecture IT requirements which an IC IT SoCC cannot fulfill, the IC element must notify the IC Chief Information Officer (IC CIO) of the requirement before adopting an IC element-centric solution.

b. In instances where there is an IC IT SoCC and an IC element asserts it has unique mission IT requirements (e.g., critical, urgent, operational impact, etc.) which an IC IT SoCC cannot fulfill, the IC element must notify the Deputy Director of National Intelligence for Intelligence Integration (DDNI/II) of the requirement before adopting an IC element-centric solution.

2. IC elements must understand and accept the shared risks of operating in an interconnected environment.

3. The IC IE, and the activities conducted therein, shall support the protection of civil liberties and privacy in accordance with applicable legal and policy requirements.

E. IC IT SERVICE PROVIDER MODEL

1. The IC will use a Service Provider model for the provisioning, funding, and use of designated IC IT SoCC. The IC IT Service Provider model consists of two roles:

a. *IC IT Service Provider* (IC IT SP) - IC elements designated by the DNI or the Principal Deputy Director of National Intelligence (PDDNI), in consultation with the affected heads of the IC elements, to develop and maintain an IC IT capability as a SoCC in accordance with ES 00960, *Designation of Services of Common Concern*, or successor policy.

b. *IC IT Service Consumer* (IC IT SC) - IC elements, or other authorized users, whose IT systems use an IC IT SoCC, and the information within, to support its mission in accordance with applicable laws, regulations, and policies.

2. The IC IT SP will coordinate with the appropriate Office of the Director of National Intelligence (ODNI) components and IC elements to deliver the IC IT SoCC via centralized, distributed, or franchised delivery models. When needed, other delivery models may be employed on a case-by-case basis. The PDDNI will provide final approval of the delivery model based on a recommendation from the appropriate IC element Deputies.

3. The IC IT SP will coordinate with appropriate ODNI components and IC elements to develop the IC IT SoCC cost and funding model which may include centralized or distributed funding, or fee-for-service. When needed, other cost and funding models may be employed on a case-by-case basis. The PDDNI will provide final approval of the model based on a recommendation from the DEXCOM.

4. IC IT SPs will prioritize and implement mission, infrastructure, and enterprise architecture capability requirements in collaboration with DDNI/II, IC CIO, and IC elements.

F. INFORMATION SHARING, SAFEGUARDING AND MANAGEMENT

1. IC elements shall use the IC IE to make information readily discoverable by and appropriately retrievable to the IC in accordance with ICD 501, *Discovery and Dissemination or Retrieval of Information within the IC.*

2. Authorized users shall access, discover, and use information in the IC IE in accordance with their approved mission needs and applicable legal and policy requirements, to include the protection of civil liberties and privacy.

3. IT capabilities will support access for authorized foreign entities to the IC IE consistent with ICD 403, *Foreign Disclosure and Release of Classified National Intelligence* and other applicable policies. Access by Second Party Integrees is governed by ES 2016-00816, *Second Party Integree Access to the IC IE.*

4. Consistent with EO 13526, IC elements shall retain their Original Classification and Declassification Authority and processes to derivatively classify, sanitize, or downgrade information under applicable legal and policy requirements. Such information shall be protected through the Originating Element's application of appropriate Original Classification Authority and derivative classification, control markings, dissemination, and technical specifications. For the purposes of this ICD, an Originating Element is defined as an IC element or U.S. government entity that creates or collects information during the course of its business and is legally responsible for it.

5. The IC IE will protect sources, methods, and intelligence information from unauthorized disclosures and insider threat, and it will mitigate counterintelligence and security risks through implementation of the *National Insider Threat Policy*, EO 13587, ICD 701, *Deterrence, Detection, Reporting, and Investigation of Unauthorized Disclosures of Classified National Security Information*, ICD 750, *Counterintelligence Programs*, and other applicable security and counterintelligence policies.

G. INFORMATION TECHNOLOGY

1. IT capabilities and infrastructures will support classification markings, access, and dissemination controls.

2. IT capabilities and infrastructures requiring interconnections with other network security domains will do so using cross-domain interfaces in coordination with relevant stakeholders.

3. IC elements will migrate to an information-centric architecture to the greatest extent possible.

4. IC IT SoCC architecture will be based on commonly designed and coherently engineered enterprise-level IT components and infrastructure that separates information from applications, services, and processes. Information separation will be achieved through a logical construct instead of by a physical separation to the greatest extent possible.

5. IC elements shall first use an IC enterprise solution for cloud storage and computing capabilities before acquiring IC element-centric data storage capabilities, including data centers. Legacy or inefficient data storage will be decommissioned to the maximum extent possible.

6. IC elements will develop and implement a strategy for managing the privacy and security risks associated with connecting separately authorized information systems within the IC IE

consistent with ICD 503, *Intelligence Community Information Technology Systems Security Risk Management.*

7. IT capabilities shall adhere to and implement approved IT standards and technical specifications for identity management, attribute-based access control, user activity monitoring and auditing, and data tagging.

8. Programming and budgeting of IC IE resources and IT capability requirements will be conducted in accordance with ICD 116, *Intelligence Planning, Programming, Budgeting, and Evaluation System* and ICD 115, *IC Capability Requirements Process.*

9. IC IE acquisition and procurement will be conducted in accordance with ICD 801, *Acquisition.*

H. ROLES AND RESPONSIBILITIES

1. The DNI or PDDNI will:

a. Designate IC elements, in consultation with the affected heads of the IC elements, as an IC IT SP to develop and maintain an IT capability as a SoCC and will define the nature and scope of the IC IT service at the time of designation;

b. Provide oversight and strategic guidance for procurement, acquisition, and funding decisions related to IC IT SoCCs; and

c. Approve the consolidated IC IE governance framework recommended by the DEXCOM.

2. The DDNI/II shall:

a. Collaborate with IC IT SPs and IC elements on prioritization of IC IT SoCC mission requirements;

b. Monitor delivery and implementation of IC IT SoCC mission requirements;

c. Respond to and track notifications of unique mission IT requirements requiring IC element-centric solutions in coordination with IC CIO;

d. Jointly develop and maintain with the IC CIO, and in coordination with ODNI component heads, a consolidated and integrated IC IE governance structure which accounts for mission, infrastructure, and enterprise architecture oversight within 60 days of the issuance of this Directive. The PDDNI will provide final approval of the governance framework based on a recommendation from the DEXCOM; and

e. Establish and maintain efficient processes for assessing the cost-benefit and implementation of changes to IC IE mission IT standards in coordination with the Assistant Director of National Intelligence (ADNI) for Systems and Resource Analyses (SRA) and IC elements.

3. The IC CIO shall:

a. Collaborate with IC IT SPs and IC elements on prioritization of IC IT SoCC infrastructure and enterprise architecture requirements;

b. Monitor delivery and implementation of IC IT SoCC infrastructure and enterprise architecture requirements;

c. Respond to and track notifications of unique infrastructure and enterprise architecture IT requirements requiring IC element-centric solutions in coordination with DDNI/II;

d. Issue standards and guidance related to the IC IE in accordance with ICD 101, *IC Policy System* and ICD 500, *Director of National Intelligence Chief Information Officer*;

e. Jointly develop and maintain with DDNI/II, and in coordination with ODNI component heads, a consolidated and integrated IC IE governance structure which accounts for mission, infrastructure, and enterprise architecture oversight within 60 days of the issuance of this Directive. The PDDNI will provide final approval of the governance framework based on a recommendation from the DEXCOM;

f. Establish and maintain efficient processes for assessing the cost-benefit and implementation of changes to IC IE infrastructure and enterprise architecture IT standards in coordination with the ADNI/SRA and IC elements; and

g. Jointly oversee acquisitions and procurements related to IC IT SoCCs with the ADNI for Acquisition, Technology, and Facilities (AT&F) through processes such as the ODNI Acquisition Review Board, Executive Program Management Reviews, and Quarterly Program Reviews.

4. The Director of the National Counterintelligence and Security Center shall issue standards and guidance related to counterintelligence and security activities in the IC IE in accordance with ICD 101.

5. ADNI/AT&F shall:

a. Jointly oversee acquisitions and procurements related to IC IT SoCCs in coordination with IC CIO through processes such as the ODNI Acquisition Review Board, Executive Program Management Reviews, and Quarterly Program Reviews;

b. Lead the consolidation, negotiation, and execution of IC Enterprise License Agreements in consultation with and on behalf of IC elements;

c. Develop standardized contract language, in coordination with IC CIO, for IC elements to use to ensure vendors comply with the appropriate provisions of this Directive; and

d. Issue standards and guidance related to acquisition and procurement in the IC IE not otherwise covered by IC CIO authorities in ICD 101 and ICD 500.

6. The Civil Liberties, Privacy and Transparency Officer shall coordinate with counterpart IC offices of privacy and civil liberties, ODNI components, and other stakeholders to ensure implementation of the IC IE, and the activities conducted therein, maintain the protection of civil liberties and privacy in accordance with applicable legal and policy requirements while enabling intelligence integration and responsible information sharing and safeguarding.

7. IC elements shall:

a. Migrate IC IT capabilities to IC IT SoCCs as quickly and efficiently as possible;

b. Provide IC IT SoCC mission, infrastructure, and enterprise architecture requirements to the IC IT SPs, in collaboration with DDNI/II and IC CIO, and support the prioritization of requirements;

c. Collaborate on and coordinate IC IT activities through the IC IE governance framework;

d. Coordinate with IC IT SPs to develop training on IC IT mission capabilities, and use of the data within the IC IT SoCC, to include compliance with legal, regulatory, and policy requirements as appropriate;

e. Ensure that all personnel accessing the IC IE have unique, identifiable identities, which can be authenticated and have current and accurate attributes for accessing information in accordance with IC policies, guidance, and specifications for identity and access management;

f. Plan, budget, and implement cost, funding, and delivery models for IC IT SoCCs in coordination with IC CIO, AT&F, the Chief Financial Officer (CFO), DDNI/II, SRA, and IC IT SPs; and

g. Apply an IC enterprise approach to acquisition and procurement needs in coordination with IC CIO, AT&F, and affected IC IT SPs.

8. IC IT Service Providers shall:

a. Manage their designated IC IT SoCC consistent with the oversight and strategic guidance provided by the DNI;

b. Deliver IC IT SoCC capability requirements in a timely manner;

c. Implement agreed upon IC IT infrastructure, enterprise architecture, and mission IT capability requirements for processing and protecting information provided by Originating Elements so that it may be made available by or through IC IT SoCCs to IC IT SCs;

d. Support the records management responsibilities of Originating Elements by providing a means to audit, track, manage, and dispose of information as required by applicable legal and policy requirements, and coordinate with Originating Elements prior to dispositioning or destroying information;

(1) The IC IT SP will not be deemed to collect, disseminate, retain, dispose, or destroy information solely by the virtue of hosting or providing system support to information that originated with another IC element;

e. Provide IC IT SCs responsive and comprehensive technical support and operational awareness related to the Service provided;

f. Coordinate with SC to develop training on IC IT mission capabilities, and use of the data within the IC IT SoCC, to include compliance with legal, regulatory, and policy requirements, as appropriate;

g. Establish cost, funding, and delivery models in coordination with IC CIO, AT&F, CFO, DDNI/II, SRA, IC IT SC, and IC elements; and

h. Apply an IC enterprise approach to acquisition and procurement needs in coordination with IC CIO, AT&F, IC IT SC, and affected IC elements.

9. Originating Elements shall:

a. Define and provide the rules for the discovery, access, use, dissemination, and retention of their information (to include U.S. Person protections as directed by EO 12333, as amended) to IC elements and IC IT SPs;

b. Determine classification and dissemination controls in accordance with EO 13587 and other legal and policy requirements;

c. Perform records management responsibilities with respect to the information they originate (e.g., *Federal Records Act*, *Freedom of Information Act*, *Privacy Act*, Office of Management and Budget/National Archives and Records Administration memoranda, M-12-18, *Managing Government Records Directive* or superseding policy, and M-14-16, *Guidance on Managing Email or superseding policy, and record retention schedules*). Records management responsibilities for joint products shall be determined by agreements among the authoring organizations;

d. Ensure data is properly tagged with accurate metadata and in accordance with IC data standards to enable reliable and accurate use of the information; and

e. Designate an IC element as a Data Custodian, as appropriate. A Data Custodian is an IC element that, on behalf of the Originating Element, may perform mission and business data-related tasks such as collecting, tagging, and processing data, and grant individual users access to additional information beyond that of general systems, applications, and file permissions to perform such functions, where appropriate.

I. EFFECTIVE DATE: This Directive becomes effective on the date of signature.

Director of National Intelligence

19 JAN 2017

Date

National Security Archive,

Suite 701, Gelman Library, The George Washington University,

2130 H Street, NW, Washington, D.C., 20037,

Phone: 202/994-7000, Fax: 202/994-7005, nsarchiv@gwu.edu