

OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE
WASHINGTON, DC 20511

NOV 25 2015

Steven Aftergood
Federation of American Scientists
1725 DeSales Street NW, Suite 600
Washington, DC 20036

Reference: ODNI Case DF-2015-00312

Dear Mr. Aftergood:

This responds to your FOIA request dated 4 September 2015 (Enclosure 1) to the Office of the Director of National Intelligence (ODNI). You requested a copy of E/S 00564, Guiding Principles for Implementing and Operating in a Common Intelligence Community Information Technology Enterprise, signed 19 September 2013.

Your request has been processed in accordance with the Freedom of Information Act (FOIA) 5 U.S.C. § 552, as amended. In response to your request, we have located the document you asked for. Upon thorough review, the ODNI has determined that this document may be released in its entirety (Enclosure 2).

If you have any questions, feel free to email our Requester Service Center at DNI-FOIA@dni.gov or call us at (703) 874-8500.

Sincerely,


Jennifer Hudson

Director, Information Management Division

Enclosures

DIRECTOR OF NATIONAL INTELLIGENCE
WASHINGTON, DC 20511

ES 00564

MEMORANDUM FOR: Distribution

SUBJECT: (U) Guiding Principles for Implementing and Operating in a
Common Intelligence Community Information Technology
Enterprise

A. (U) Introduction

1. (U) To improve the ability to securely and efficiently discover, access, and share information, the Intelligence Community (IC) will store, process, and retain intelligence and intelligence-related information collected and obtained; conduct analysis; and disseminate product on the common information technology environment, Intelligence Community Information Technology Enterprise (IC ITE).

2. (U) Implementation of IC ITE is a complex and iterative process of consolidating Community capabilities and resources. The following principles form the policy framework for operation and maintenance of IC ITE and the activities within the environment when fully operational and therefore will guide the implementation process and related activities.

3. (U) Initial stages of implementation will focus on the establishment of IC ITE as infrastructure that provides end-to-end means for storing, processing, retaining, analyzing, and disseminating intelligence and intelligence-related information under current IC policies and practices. After initial deployment of the operational baseline, there will be a focus on advancing intelligence integration through more effective information sharing and safeguarding, thereby enabling deeper analytic collaboration across all IC Elements.

4. (U) IC ITE is being established as a TS/SCI environment, but shall interconnect with and support other domains through the use of cross-domain interfaces.

5. (U) Implementation of the common environment and the activities conducted therein shall maintain the protection of civil liberties and privacy while enabling intelligence integration and responsible information sharing and safeguarding. Implementation shall also be consistent with Federal statutes, Executive Orders, Presidential Directives, Attorney General-approved guidelines, IC policy, and IC element policies that do not otherwise conflict with these requirements (hereinafter, applicable legal and policy requirements).

6. (U) IC elements shall abide by each principle provided below with exemptions being granted by the Director of National Intelligence or Principal Deputy Director of National Intelligence on a case-by-case basis. Implementation shall be consistent with IC policy, including ICD 501, *Discovery and Dissemination or Retrieval of Information within the Intelligence Community*, regarding data access and management and ICD 503, *IC Information Technology Systems Security Risk Management, Certification and Accreditation*, with respect to risk management.

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~

SUBJECT: (U) Guiding Principles for Implementing and Operating in a Common Intelligence Community Information Technology Enterprise

B. (U//~~FOUO~~) Architecture

1. (U//~~FOUO~~) IC ITE architecture utilizes a service model for the provision of IT. IC ITE architecture will provide commonly designed and coherently engineered enterprise-level IT components and infrastructure based upon the following operating principles:

a. The default approach for development, acquisition, and implementation of IT tools, products, and services shall be to build and operate in common.

b. Core IT services will be provided by Service Providers, designated by the DNI in consultation with affected IC element heads. Implementation will be achieved through formal designation and completion of a Memorandum of Understanding (MOU) outlining terms of performance.

c. Information sharing and safeguarding within IC ITE shall be supported by a common framework for identity management, attribute-based access control, user activity auditing and monitoring, and data tagging.

d. Secure communities of interest and secure collaborative environments established prior to the effective date of these Principles shall be transferred into and supported by IC ITE, to the greatest extent possible and in accordance with A.6 above.

e. Implementation of IC ITE will be achieved through the development and deployment of the following services (hereinafter, IC ITE Services):

- (1) a common desktop environment;
- (2) a joint cloud environment;
- (3) an applications mall;
- (4) enterprise management capability;
- (5) identification, authentication, and authorization capabilities;
- (6) network requirements and engineering services, and
- (7) a security coordination service.

2. (U) Configuration management of IC ITE shall be conducted through a process for identifying and prioritizing changes to the baseline, configuration item identification, change control, and configuration audits. The IC ITE enterprise management service provider, in coordination with the IC CIO, shall establish and maintain a process for the implementation of changes to IC ITE. Changes made to the enterprise shall follow standard methods, processes, and procedures as directed by the IC CIO in order to facilitate efficient and prompt resolution.

3. (U//~~FOUO~~) Any necessary separation of data within IC ITE shall be achieved through a logical construct instead of by physical separation to the greatest extent possible and in accordance with applicable legal and policy requirements and Section A.6 above.

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~

SUBJECT: (U) Guiding Principles for Implementing and Operating in a Common Intelligence Community Information Technology Enterprise

C. (U//FOUO) Access, Use, and Discovery – Information acquired, collected, or produced by IC elements shall be available for access for all IC missions and functions, subject to applicable legal and policy requirements. Determinations about access to and use of such information within IC ITE shall continue to be based upon content and mission need.

1. Access – Access to data within IC ITE shall be determined by information protection profiles, user clearance, and need to know criteria established by originators of intelligence information in accordance with IC policy.

a. Access to data within IC ITE shall comply with applicable legal and policy requirements governing this data.

b. Access controls shall be enforced by the system processes in accordance with established rules.

c. Access logs will be maintained and audited in accordance with established rules.

d. IC ITE will support the requirements for access by foreign nationals (to include Second Party nationals accessing non-partnership systems) to systems processing intelligence information consistent with DCID 6/3, Appendix E, *Access by Foreign Nationals To Systems Processing Intelligence Information*.

2. Use – Use of intelligence information within IC ITE shall be pursuant to an authorized recipient's mission need in accordance with applicable legal and policy requirements governing the recipient's own missions and functions.

3. Discovery

a. Consistent with ICD 501, unless a discovery exemption has been obtained, originating IC elements shall authorize and provide for automated discovery and retrieval of intelligence and intelligence-related information in IC ITE by authorized personnel meeting access criteria in a manner that complies with applicable legal and policy requirements.

b. IC elements that acquire or hold information provided by consent or by arrangement or agreement with federal departments or agencies, foreign nations, organizations, corporations, state, local, or tribal entities, or individuals outside the IC shall seek consent to make the information discoverable and retrievable in IC ITE. IC elements party to such agreements shall coordinate with the ODNI to seek to negotiate future agreements that provide for storage, processing, and retention within IC ITE.

D. (U) Information Management – The creation, handling, use, protection, and disposition of intelligence information in IC ITE shall comply with applicable legal and policy requirements.

1. Classification and Declassification – Consistent with EO 13526, *Classified National Security Information*, IC elements retain their Original Classification Authority within IC ITE. IC ITE does not alter classification, declassification, sanitization or downgrade authorities or responsibilities under applicable legal and policy requirements.

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~

SUBJECT: (U) Guiding Principles for Implementing and Operating in a Common Intelligence Community Information Technology Enterprise

2. **Records Management – Originating Elements** retain their records management responsibilities within IC ITE with respect to the information they originate (e.g., Federal Records Act, Freedom of Information Act, Privacy Act, and record retention schedules). To enable originators to fulfill these records management responsibilities, IC ITE Service Providers shall provide the means to audit, track, manage, and if necessary, purge information as required by applicable legal and policy requirements.

3. **Joint Products – Records management responsibilities for joint products** shall be documented by the authoring IC elements.

4. **Data Governance – Consistent with guidance issued by the IC CIO**, data within IC ITE shall be tagged and marked with sufficient fidelity so that it may be stored, processed, retained, handled, and disseminated in full compliance with applicable legal and policy requirements, including Federal statutes, regulations, Executive Orders, Presidential Directives, court orders, Attorney General–approved guidelines and other authorities regarding retention and dissemination, including retention and dissemination of U.S. Person information.

E. (U//~~FOUO~~) Systems Security

1. The IC CIO is the assessing and authorizing official for IC ITE Services and components and provides the framework for security control assessments and authorization decisions for IC ITE, in consultation with Service Providers and affected IC elements.

2. IC elements developing applications connecting to and using IC ITE services shall be responsible for the assessment and authorization of such applications, consistent with the risk mitigation framework provided in ICD 503.

3. IC ITE will be supported by a common security risk management framework in which baseline security controls and security requirements are integrated into system requirements.

F. (U//~~FOUO~~) Personnel Security

1. IC elements shall ensure that their IC ITE users have the accurate attributes for accessing data placed in IC ITE.

2. Privileged Users within IC ITE who perform system administration functions may be subject to additional scrutiny in the performance of this role, in accordance with IC policy.

3. IC ITE shall provide mechanisms for appropriate separation of duties among those Privileged Users with the highest accesses, so that accesses and privileges are distributed across the user population and no such individuals are able to perform all privileged actions for sensitive systems or applications.

4. Personnel security processes and identity management tools will provide means for access by foreign partner detailees to the IC, consistent with DCID 6/3, Appendix E.

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~

SUBJECT: (U) Guiding Principles for Implementing and Operating in a Common Intelligence Community Information Technology Enterprise

G. (U//~~FOUO~~) Information Security

1. IC ITE will be supported by an integrated and layered security architecture that meets the requirements for providing end-to-end technical and procedural security; an integrated security model for authorized access to IC ITE information resources; capabilities to collect, share, and analyze audit data; and end-to-end encryption capabilities available to further protect the sensitive data.

2. Intelligence information shall be protected in IC ITE through application of original classification and control decisions; use of derivative classification and control markings; technical specifications on machine-readable classification and control markings; national, IC, and individual IC element policies; and adherence to standardized counterintelligence and security practices. Information in IC ITE may be tagged with attributes not covered under the *Intelligence Community Authorized Classification and Control Markings Register and Manual*, such as need to know categories, communities of interest, dissemination, and usage control policy variables.

H. (U//~~FOUO~~) Counterintelligence – IC ITE shall include comprehensive implementation of the National Insider Threat Policy, including an enterprise audit program. IC ITE Service Providers shall provide user audit and monitoring data to the gaining or employing agencies of IC ITE users and to the IC incident response and security coordination center.

I. (U//~~FOUO~~) Acquisition and Procurement – The DNI provides the strategic framework for procurement and acquisitions in support of IC ITE by:

1. Providing direction and oversight of all IC ITE procurement;
2. Ensuring that execution of budgets for enterprise information technology and enterprise-related research and development is consistent with the IC ITE strategy and these Principles;
3. Addressing and mitigating supply chain threats; and
4. Conducting oversight of acquisitions related to IC ITE Services through the DNI Acquisition Review Board chaired by the IC CIO.

J. (U) IC ITE Services – IC elements designated by the DNI as Service Providers will develop, maintain, and provide IC ITE Services of common concern.

1. The DNI will provide oversight and strategic guidance with respect to IC ITE Services.
2. The nature and scope of IC ITE Services will be defined at the time of designation. The roles and responsibilities will be captured in a DNI designation memorandum and MOU consistent with DNI guidance on the establishment of services of common concern.
3. As IC ITE operational capabilities are implemented, the cost for IC ITE Services may in some instances be centrally funded. Consumers of Services that are not centrally funded will compensate Service Providers or their contractors for the use of those Services as appropriate.

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~

SUBJECT: (U) Guiding Principles for Implementing and Operating in a Common Intelligence Community Information Technology Enterprise

4. Funding decisions for IC ITE will be made by the DNI as part of the budget and planning process, in coordination with IC element heads.

K. (U) Legal Responsibilities and Compliance Requirements

1. Each IC element participating in IC ITE retains its existing legal, regulatory, policy, and statutory responsibilities for the information that it provides to, and accesses through, IC ITE.

2. IC ITE shall enable Service Provider, Service Consumer, Originating Element, and Data Custodian compliance with their respective obligations under law and policy.

3. Each IC element remains responsible for ensuring that the provision of information to IC ITE is in accordance with applicable legal and policy requirements and other authorities applicable to the information, including those authorities regarding the retention, use, and dissemination of U.S. Person information.

4. Use of IC ITE Services represents user consent to monitoring, access, use, and disclosure of their electronic communications. Each participating agency shall ensure user consent to monitoring, access, use, and disclosure of electronic communications or data residing in IC ITE.

L. (U) Roles and Responsibilities – Within IC ITE, there are four roles: Service Provider, Service Consumer, Originating Element, and Data Custodian.

1. Service Provider – An IC element designated by the DNI, in consultation with the IC element head, to develop and maintain an IC ITE Service of common concern. Service Providers are responsible for facilitating IC elements' fulfillment of their respective information management responsibilities. A Service Provider uses only those authorities necessary to fulfill the responsibilities to manage the Service. These authorities are distinct from those of an IC element acting as an originator of intelligence information or as a consumer of the Service. When other IC elements provide intelligence information to a Service Provider so that it may be made available by or through IC ITE, the Service Provider is responsible for implementing the agreed upon policies for processing and protecting that information. (The Service Provider may provide Privileged Users access to an originating element's information, unless otherwise protected (e.g., encrypted) for administrative and technical support purposes.) However, a Service Provider does not collect, retain, purge, destroy or disseminate information solely by the virtue of hosting, or providing system support to information on IC ITE that originated with another IC element. Further, Service Providers may not purge or destroy information without prior coordination with the appropriate Originating Element.

2. Service Consumer – An organization whose affiliates and systems use the Service in accordance with its own authorities. In doing so, a Service Consumer uses the Service and any intelligence information that may be provided therein in accordance with law, regulation, and

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~

SUBJECT: (U) Guiding Principles for Implementing and Operating in a Common Intelligence Community Information Technology Enterprise

policy governing the processing and protecting of such information in the conduct of its own missions and functions, as well as potential usage restrictions by Originating Elements.

3. Originating Elements – A department, agency or component thereof that creates or collects information during the course of its business and is legally responsible for it (e.g., records management, classification, and lead for Freedom of Information Act and Privacy Act responsibilities).


a. Originating Elements make classification, access, and dissemination control determinations, and tag data for ingest into IC ITE. IC ITE will accommodate these decisions in a manner consistent with the standardized identity management, attribute-based access controls, and data tagging methodologies.

b. Originating elements perform records management activities with respect to the information they provide to IC ITE.

c. Originating Elements may delegate some of the activities listed above to an IC element to handle information on its behalf (see Data Custodian).

4. Data Custodian - An organization that is responsible for executing data-related tasks on behalf of an Originating Element. These tasks may include collecting, tagging, and processing data. An Originating Element may authorize Data Custodians to grant individual users access to additional information beyond that of general systems, application and file permissions to perform such functions.

M. (U) Policy Review – IC elements shall review their policies to ensure consistency with the Guiding Principles contained in this memorandum. These Principles provide the basis for the Community's implementation of IC ITE and will be incorporated into an IC policy issuance to govern IC activities within IC ITE after initial deployment of the operational baseline.


James R. Clapper

19 Sep 2013
Date

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~

SUBJECT: (U) Guiding Principles for Implementing and Operating in a Common Intelligence Community Information Technology Enterprise

Distribution:

Director, Central Intelligence Agency
Director, Defense Intelligence Agency
Director, National Security Agency
Director, National Reconnaissance Office
Director, National Geospatial-Intelligence Agency
Deputy Chief of Staff, G-2, U.S. Army
Director of Naval Intelligence, U.S. Navy
Deputy Chief of Staff for Intelligence, Surveillance and Reconnaissance, A2, U.S. Air Force
Director of Intelligence, U.S. Marine Corps
Executive Assistant Director, National Security Branch, Federal Bureau of Investigation
Assistant Commandant for Intelligence and Criminal Investigations, CG-2, U.S. Coast Guard
Under Secretary of Defense for Intelligence, Department of Defense
Assistant Secretary, Bureau of Intelligence and Research, Department of State
Assistant Secretary, Office of Intelligence and Analysis, Department of the Treasury
Chief, Intelligence Division, Drug Enforcement Administration
Under Secretary, Intelligence and Analysis, Department of Homeland Security
Director, Office of Intelligence and Counterintelligence, Department of Energy
Joint Staff Director for Intelligence, J2, Vice Chairman of the Joint Chiefs of Staff

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~