

UNCLASSIFIED

OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE
WASHINGTON, DC 20511

2019-090

MEMORANDUM FOR: Distribution

SUBJECT: (U) Technical Soundness Approval of Intelligence Community
Technical Specification Updates (2019-MAR Release)

REFERENCES: A. (U) Intelligence Community Directive 500, *Director of
National Security Chief Information Officer*, 7 August 2008
B. (U) Intelligence Community Standard 500-20, *Intelligence
Community Enterprise Standards Compliance*, 16 December
2010

(U) Intelligence Community (IC) policy issued by the Director of National Intelligence (e.g. reference A) calls upon the Intelligence Community Chief Information Officer (IC CIO) to establish, coordinate, and promulgate common Information Technology (IT) standards, protocols, and interfaces for and within the IC, as required, to support information sharing strategies; intelligence mission objectives established in relevant law, policy, and directives; and the IC Information Environment (IC IE).

(U) The Office of the IC CIO facilitates IC-wide collaboration and coordination bodies charged with development, modification, and governance of IC technical specifications of common concern. As the IC CIO accountable official responsible for developing and coordinating these specifications among IC element and external stakeholders, I hereby assert that the following IC Technical Specifications are technically sound, supportive of IC mission objectives and the IC IE, and are implementable as of this memorandum's signature date:

- 1) *XML Data Encoding Specification for Audit V2019-MAR* (AUDIT.XML.V2019-MAR) – This specification is revised to improve search queries.
- 2) *XML Data Encoding Specification for Data Element Definition V2019-MAR* (DED.XML.V2019-MAR) – This specification is added to the technical specifications family. This XML Data Encoding Specification for Data Element Definition (DED.XML) defines detailed implementation guidance for XML encoding of data element definition data.
- 3) *XML Data Encoding Specification for IC Enterprise Data Header V2019-MAR* (IC-EDH.XML.V2019-MAR) – This specification is revised with incorporating the changes to ISM/ARH/NTK and the new IC-SF specification.
- 4) *Secret Entity Attributes for the Intelligence Community V2019-MAR* (IC-SEA.XML.V2019-MAR) – This specification is added to the technical specifications family. This specification governs the set of IC enterprise secret

UNCLASSIFIED

SUBJECT: (U) Technical Soundness Approval of Intelligence Community Technical Specification Updates (2019-MAR Release)

entity attributes and associated values that must be supported by an Attribute Service participating in the IC's Unified Authorization and Attribute Services capability.

- 5) *Attribute Practice Compliance Statements for the IC Secret Fabric V2019-MAR* (IC-SEA-APCS.V2019-MAR) – This specification is added to the technical specifications family. This specification provides concise direction to produce an attribute practice statement for each attribute service of an IC element for use by the secret fabric instantiation of C2S. Compliance with the APCS document ensures interoperability and consistently applied attributes in dynamic IT environments.
- 6) *Intelligence Community Specification Framework V2019-MAR* (IC-SF.XML.V2019-MAR) – This specification is added to the technical specifications family. This specification defines the basic conceptual structure and outlines the core philosophy of IC technical specifications.
- 7) *XML Data Encoding Specification for IC Trusted Data Format V2019-MAR* (IC-TDF.XML.V2019-MAR) – This specification is revised to consolidate security control specifications.
- 8) *XML Data Encoding Specification for Information Resource Metadata V2019-MAR* (IRM.XML.V2019-MAR) – This specification is revised to better represent geospatial information.
- 9) *XML Data Encoding Specification for Information Security Markings V2019-MAR* (ISM.XML.V2019-MAR) – This revision merges ARH and NTK into ISM.
- 10) *Access Control Encoding Specification for Information Security Markings V2019-MAR* (ISM.ACES.V2019-MAR) – This specification is revised to consolidate security control specifications.
- 11) *Controlled Vocabulary Encoding Specification for Information Security Marking Country codes and Tetragraphs V2019-MAR* (ISMCAT.CES.V2019-MAR) – This specification is revised to align with and utilize the new IC-SF specification.
- 12) *Taxonomy Encoding Specification for Mission Need Taxonomy V2019-MAR* (MNT.XML.V2019-MAR) – This version incorporates changes from the authoritative source.
- 13) *CVE Encoding Specification for Production Metrics V2019-MAR* (PM.CES.V2019-MAR) – This version incorporates changes from the authoritative source and adds location in support of production metric triples.
- 14) *XML Data Encoding Specification for Production Metrics Assertion V2019-MAR* (PMA.XML.V2019-MAR) – This specification is added to the technical specifications family. This specification defines a simple structured assertion for conveying sets of production metric triples using XML within a Trusted Data Format object or collection.

SUBJECT: (U) Technical Soundness Approval of Intelligence Community Technical Specification Updates (2019-MAR Release)

- 15) *Attribute Practice Compliance Statements for Unified Identity Attribute Set V2019-MAR* (UIAS-APCS.V2019-MAR) – This specification is revised to consolidate security control specifications. This specification was originally released as APCS and has been renamed to UIAS-APCS for better specificity.
- 16) *XML Data Encoding Specification for Community Shared Resources Technical Specification Profiles AUDIT v2019-MAR* (CSR-AUDIT.XML.V2019-MAR) – This specification is revised to align the AUDIT profile with the 2019-MAR specifications.
- 17) *CVE Encoding Specification for Geopolitical Entities, Names, and Codes v2019-MAR* (IC-GENC.CES.V2019-MAR) – This specification is revised to align with GENC Edition 3 Updates 8 and 9.
- 18) *CVE Encoding Specification for Fine Access Control v2019-MAR* (FAC.CES.V2019-MAR) – This specification is revised to incorporate new SCI information from the authoritative source.
- 19) *Controlled Vocabulary Encoding Specification for Mission Need v2019-MAR* (MN.CES.V2019-MAR) – This version incorporates changes from the authoritative source.
- 20) *Whitelist Guidance for ISM* (Whitelist.XML.v2019-MAR). This specification is included for awareness purposes only. It is not a signed artifact.

(U) NOTIFICATION: The rules for RD/CNWDI are not updated in the ISM.ACES.V2019-MAR specification per changes in the 2018 RD errata to the 2016 Register and Manual. Due to inconsistent policy that is not machine implementable, the IC CIO technical specifications were granted exemption from updating the most recent changes for RD/CNWDI as described in the Register. DOE committed to resolving this policy issue as soon as possible to ensure that DOE data is adequately shared and protected in the enterprise.

(U) In accordance with reference B, these IC Technical Specifications are approved for submission to the IC Enterprise Standards Baseline (IC ESB) which serves as the collection of enterprise standards against which programs will be assessed for IC Enterprise Architecture compliance. The IC Technical Specifications can be accessed at <http://go.ic.gov/RxSUraG> on Intelink-TS and <http://www.w3id.org/ic/standards/final> on Intelink-U.

UNCLASSIFIED

SUBJECT: (U) Technical Soundness Approval of Intelligence Community Technical Specification Updates (2019-MAR Release)

(U) This memorandum becomes effective on the date of signature.



Susan T. Dorr
Director, Cybersecurity Division &
Intelligence Community Chief Information Security Officer

23 April 2019
Date

Attachments:

1. (U) *IC Technical Specification Mapping to IC/DoD Guidance (2019-MAR Release)*

UNCLASSIFIED

SUBJECT: (U) Technical Soundness Approval of Intelligence Community Technical Specification Updates (2019-MAR Release)

Distribution:

Chief Information Officer, Central Intelligence Agency
Chief Information Officer, Defense Intelligence Agency
Chief Information Officer, Federal Bureau of Investigation
Chief Information Officer, National Geospatial-Intelligence Agency
Chief Information Officer, National Reconnaissance Office
Chief Information Officer, National Security Agency
Chief Information Officer, Office of the Director of National Intelligence
Chief Information Officer, Intelligence Division, Drug Enforcement Administration
Chief Information Officer, Office of Intelligence and Counterintelligence, Department of Energy
Chief Information Officer, Intelligence and Analysis, Department of Homeland Security
Chief Information Officer, Bureau of Intelligence and Research, Department of State
Chief Information Officer, Office of Intelligence and Analysis, Department of the Treasury
Deputy Chief of Staff, G-2, U.S. Army
Assistant Commandant for Intelligence and Criminal Investigations, CG-2, U.S. Coast Guard
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
Assistant Secretary of Defense for Networks and Information Integration/Chief Information Officer, U.S. Department of Defense
Under Secretary of Defense for Intelligence

Policy Trace

Table 1 - Policy Trace Matrix

	AUDIT	CSR-AUDIT	DED	FAC-CES	IC-EDH	IC-GENC	IC-SEA	IC-SEA-APCS	IC-SF	IC-TDF	IRM	ISM	ISM-ACES	ISM-CAT-CES	MN-CES	MNT	PM-CES	PMA	UIAS-APCS
500 Series:																			
ICD 500, Director Of National Intelligence Chief Information Officer	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
ICD 501, Discovery and Dissemination or Retrieval of Information within the IC		X		X	X	X	X	X		X	X	X	X	X	X	X	X	X	X
ICD 502, Integrated Defense of the Intelligence Community Information Environment	X						X	X											
ICD 503, Intelligence Community Information Technology Systems Security Risk Management	X																		
ICPG 500.1, Digital Identity																			X
ICPG 500.2, Attribute-based Authorization and Access Management							X	X	X										X
ICS 500-20, IC Enterprise Standards Compliance	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
ICS 500-21, Tagging of Intelligence and Intelligence-Related Information				X	X	X				X	X	X	X	X					
ICS 500-27, Collection and Sharing of Audit Data	X						X	X											X
ICS 500-29, IC Digital Identifier																			X
ICS 500-30, Enterprise Authorization Attributes: Assignment, Authoritative Sources, and Use for Attribute-Based Access Control of Resources																			X
200 Series:																			
ICD 206, Sourcing Requirements for Disseminated Analytic Products						X					X								
ICD 208, Write for Maximum Utility				X	X	X				X	X	X	X	X					
ICD 209, Tearline Production and Dissemination				X	X	X				X	X	X	X	X					
ICPM 2007-200-2, Preparing Intelligence to Meet the Intelligence Community’s Responsibility to Provide		X		X	X	X				X	X	X	X	X					
700 Series:																			
ICD 710, Classification and Control Markings System				X								X	X	X					

	AUDIT	CSR-AUDIT	DED	FAC-CES	IC-EDH	IC-GENC	IC-SEA	IC-SEA-APCS	IC-SF	IC-TDF	IRM	ISM	ISM-ACES	ISM-CAT-CES	MN-CES	MNT	PM-CES	PMA	UIAS-APCS
ICPG 710.1, Application of Dissemination Controls: Originator Control				X								X	X	X					
ICPG 710.2, Application of Dissemination Controls: Foreign Disclosure and Release Markings												X							
ICS 700-2, Use of Audit Data for Insider Threat Detection	X																		
ICPG 704.5, Intelligence Community Security Database Scattered Castles																			X
100 Series:																			
ICD 121, Managing the Intelligence Community Information Environment							X	X											X
Memorandums:																			
OMB Memo - Continued Implementation of Homeland Security Presidential Directive (HSPD) 12 – Policy for a Common Identification Standard for Federal Employees and Contractors							X	X											X
IC CIO Memo - Improving Intelligence Community (IC) Identity, Credential, and Access Management (ICAM) to Achieve Greater Mission Effectiveness							X	X											X
Federal Regulations:																			
Federal Identity, Credential, and Access Management (FICAM) Roadmap and Implementation Guidance							X	X											
Executive Orders:																			
Executive Order 13526 Classified National Security Information												X	X						
Executive Order 13556 Controlled Unclassified Information												X	X						
Presidential Directives																			
HSPD-12Homeland Security Presidential Directive 12: Policy for a Common Identification Standard for Federal Employees and Contractors							X	X											X
Implementing Directives:																			
32 CFR Parts 2001 and 2003Classified National Security Information; Final Rule												X	X						
32 CFR Parts 2002Controlled Unclassified; Final Rule												X	X						

	AUDIT	CSR-AUDIT	DED	FAC-CES	IC-EDH	IC-GENC	IC-SEA	IC-SEA-APCS	IC-SF	IC-TDF	IRM	ISM	ISM-ACES	ISM-CAT-CES	MN-CES	MNT	PM-CES	PMA	UIAS-APCS
32 CFR Parts 2003The Interagency Security Classification Appeals Panel (ISCAP) Bylaws, Rules, and Appeal Procedures												X	X						
32 CFR Parts 2004National Industrial Security Program Directive No. 1												X	X						
CNSS:																			
CNSS Directive No. 506: National Directive to Implement Public Key Infrastructure for the Protection of Systems Operating on Secret Level Networks							X	X											
CNSS Directive No. 507: National Directive for Identity, Credential and Access Management Capabilities (ICAM) on the United States Federal Secret Fabric							X	X											
CNSS White Paper 01-14: Federal Identity, Credential, and Access Management (FICAM) Planning Guidance for the Secret Fabric							X	X											
CNSS Policy 25: National Policy for Public Key Infrastructure in National Security Systems							X	X											
CNSSI 1300: Instruction for National Security Systems Public Key Infrastructure X.509 Certificate Policy Under CNSS Policy No. 25							X	X											