

UNCLASSIFIED

OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE
IC CHIEF INFORMATION OFFICER
WASHINGTON, DC

2021-0660

MEMORANDUM FOR: Distribution

SUBJECT: Technical Soundness Approval of Intelligence Community
Technical Specification Updates (2021-NOV Release)

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

Reference A requires the Intelligence Community Chief Information Officer (IC CIO) to establish, coordinate, and promulgate common information technology standards, protocols, and interfaces for and within the IC, as required, to support: 1) information-sharing strategies, 2) intelligence mission objectives established in relevant law, policy, and directives, and 3) the IC information environment (IC IE).

The Office of the IC CIO facilitates IC-wide collaboration and coordination with entities 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 elements and external stakeholders, I hereby assert that the following IC technical specifications are technically sound and supportive of IC mission objectives and the IC IE. These IC technical specifications are implementable as of this memorandum's signature date:

- 1) XML Data Encoding Specification for Analysis Assertion, V2021-NOV (ANLYS.XML.V2021-NOV)—this new specification provides a way to capture analytical information such as analysis of digital hazardous materials or cross-domain transfers. The specification tracks information such as the file being analyzed, the methods, tools, and results of the analysis, analyst identifiers, attack ids, workflow ids, and if the payload is known to be malicious.
- 2) XML Data Encoding Specification for Audit, V2021-NOV (AUDIT.XML.V2021-NOV)—this specification is being revised to add support for EDH Security element constraints.
- 3) XML Data Encoding Specification for Trusted Data Format–Base, V2021-NOV (BASE-TDF.XML.V2021-NOV)—this specification is being revised to allow hash elements in ReferenceValueType independent of blocking.
- 4) XML Data Encoding Specification for Cross Domain System Manifest Assertion, V2021-NOV (CDSM.XML.V2021-NOV)—this specification is being revised to use the ANLYS.XML specification for analysis assertions.

UNCLASSIFIED

SUBJECT: Technical Soundness Approval of Intelligence Community Technical Specification Updates (2021-NOV Release)

- 5) XML Data Encoding Specification for Cross Domain System Manifest TDF, V2021-NOV (CDSM-TDF.XML.V2021-NOV)—this specification is being revised to use the ANLYS.XML specification for analysis assertions.
- 6) XML Data Encoding Specification for Community Shared Resources Technical Specification Profiles AUDIT, V2021-NOV (CSR-AUDIT.V2021-NOV)—this specification is being revised to remain aligned with changes being made to the AUDIT.XML specification.
- 7) XML Data Encoding Specification for DigitalHazMat Assertion, V2021-NOV (DHZM.XML.V2021-NOV)—this specification is being revised to use the ANLYS.XML specification for analysis assertions.
- 8) XML Data Encoding Specification for DigitalHazMat TDF, V2021-NOV (DHZM-TDF.XML.V2021-NOV)—this new specification is a minimized profile of TDF, providing non-repudiation, obfuscation, and secure cross-domain transfer of digital hazmat across the various domains in the enterprise for provenance and analysis.
- 9) XML Data Encoding Specification for DigitalHazMat Commercial TDF, V2021-NOV (DHZMC-TDF.XML.V2021-NOV)—this specification is being revised to use the ANLYS.XML specification for analysis assertions.
- 10) XML Data Encoding Specification for Document and Media Exploitation, V2021-NOV (DOMEX.XML.V2021-NOV)—this specification is being revised to remove references to the DDMS standard which has been subsumed into IRM.XML.
- 11) CVE Encoding Specification for Fine Access Control, V2021-NOV (FAC.CES.V2021-NOV)—this specification is being revised to align with the August 2019 version of the IC Markings Register and Manual.
- 12) Data Encoding Specification for IC Full Service Directory Schema, V2021-NOV (FSD.V2021-NOV)—this specification is being revised to format the UIAS.XML foreign partner organizations to match IC-SEA and 5EE.
- 13) CVE Encoding Specification for Geopolitical Entities, Names, and Codes, V2021-NOV (IC-GENC.XML.V2021-NOV)—this specification is being revised to better align the documentation with the appropriate policy.
- 14) XML Data Encoding Specifications for Intelligence Community Identifier, V2021-NOV (IC.ID.XML.V2021-NOV)—this specification is being revised to align with and utilize the IC-SF.XML framework and to remove its dependency on ISM.
- 15) Intelligence Community Specification Framework, V2021-NOV (IC-SF.XML.V2021-NOV)—this specification is being revised to update the documentation with the addition of several new specifications.
- 16) XML Data Encoding Specification for IC Trusted Data Format, V2021-NOV (IC-TDF.XML.V2021-NOV)—this specification is being revised to use the BASE-TDF.XML specification.
- 17) XML Data Encoding Specification for Information Resource Metadata, V2021-NOV (IRM.XML.V2021-NOV)—this specification is being revised to better represent geospatial information.
- 18) XML Data Encoding Specification for Information Security Markings, V2021-NOV (ISM.XML.V2021-NOV)—this specification is being revised to incorporate Controlled Unclassified Information (CUI) markings and to align with the new ROLE.CES and ISM-Rollup.XML and updated FAC.CES specifications.

SUBJECT: Technical Soundness Approval of Intelligence Community Technical Specification Updates (2021-NOV Release)

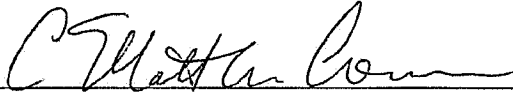
- 19) Access Control Encoding Specification for Information Security Markings, V2021-NOV (ISM.ACES.V2019- MAR)—this specification is being revised to align with the new ROLE.CES and updated FAC.CES specifications.
- 20) CVE Encoding Specification for ISM Country Codes and Tetragraphs, V2021-NOV (ISMCAT.CES.V2021-NOV)—this specification is being revised to align with the tetragraphs and organizational codes from Partner Engagement.
- 21) CVE Encoding Specification for Mission Need, V2021-NOV (MN.CES.V2021-NOV)—this specification is being revised to align with and utilize the IC-SF.XML framework and to add ANAN for Regions and ANY for Issue.
- 22) XML Data Encoding Specification for Revision Recall, V2021-NOV (RevRecall.XML.V2021-NOV)—this specification is being revised to align with and utilize the IC-SF.XML framework and to align with ICPM 200-01, which supersedes the memorandum for distribution signed by Director of National Intelligence Negroponte on 5 August 2005, of the same name.
- 23) CVE Encoding Specification for Role, V2021-NOV (ROLE.CES.V2021-NOV)—this new specification uses XML to define the permissible values for representing Roles using XML. Role is an attribute within UIAS.XML specification. This version enables use of different versions of the specifications it is dependent on, allowing them to evolve independently.
- 24) IC Enterprise Attribute Exchange Between IC Attribute Services Unified Identity Attribute Set, V2021-NOV (UIAS.XML.V2021-NOV)—this specification is being revised to align with the new ROLE.CES specification and to align with the August 2019 version of the IC Markings Register and Manual.
- 25) Attribute Practice Compliance Statements for Unified Identity Attribute Set, V2021-NOV (UIAS-APCS.V2021-NOV)—this specification is being revised to align with the August 2019 version of the IC Markings Register and Manual.
- 26) CVE Encoding Specification for US Agency Acronyms V2021-NOV, (USAgency.CES.V2021-NOV). This specification is being revised to align with and utilize the IC-SF.XML framework, to format the UIAS.XML foreign partner organizations to match IC-SEA and SEE, and to add the new U.S. Space Force (USSF).
- 27) Roll-up Guidance for ISM, V2021-NOV (ISM-Rollup.XML.V2021-NOV)—this specification is included for awareness purposes only. It is not a signed artifact.

In accordance with reference B, the 2021-NOV version of the IC technical specifications are approved for submission to the IC Enterprise Standards Baseline, 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 <https://w3id.org/ic/standards/final> on Intelink-U.

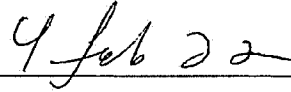
UNCLASSIFIED

SUBJECT: Technical Soundness Approval of Intelligence Community Technical Specification Updates (2021-NOV Release)

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



C. Matthew Conner
Director, Cybersecurity Group and
Intelligence Community Chief Information Security Officer



Date

(U) Attachment:

IC Technical Specification Mapping to IC/DoD Guidance, (2021-NOV Release)

UNCLASSIFIED

UNCLASSIFIED

SUBJECT: Technical Soundness Approval of Intelligence Community Technical Specification Updates (2021-NOV 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
Chief Information Officer, Department of Defense
Deputy Chief of Staff for Intelligence, United States Army
Director of Naval Intelligence, United States Navy
Director of Intelligence, United States Marine Corps
Assistant Commandant for Intelligence and Criminal Investigations, United States Coast Guard
Deputy Chief of Staff for Intelligence, Surveillance, Reconnaissance, and Cyber Effects Operations A2/6, United States Air Force
Chief Information Office, United States Space Force
Under Secretary of Defense for Intelligence and Security

UNCLASSIFIED

UNCLASSIFIED

IC Technical Specification Mapping to IC/DoD Guidance (2021-NOV Release)

UNCLASSIFIED

Table 1 - Policy Trace Matrix

	ANLYS	AUDIT	BASE-TDF	CDSM	CDSM-TDF	CSR-AUDIT	DH2M	DH2M-TDF	DH2MC-TDF	DOMEX	FAC-CES	FSD	IC-GENC	IC-ID	IC-SF	IC-TDF	IRM	ISM	ISM-ACES	ISM-Rollup	ISM-CAT-CES	MN-CES	ROLE-CES	RevRecall	UIAS	UIAS-APCS	USAGENCY-CES
100 Series:																											
ICD 121, Managing the Intelligence Community Information Environment																									X	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	X						
ICD 209, Tearline Production and Dissemination			X								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	X						
ICPM 200-01, Intelligence Community Standards and Procedures for Revised or Recalled Intelligence Products																								X			
300 Series:																											
ICD 302, Document and Media Exploitation										X																	
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	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	X	X	X	X	X	X	
ICD 502, Integrated Defense of the Intelligence Community Information Environment		X											X														
ICD 503, Intelligence Community Information Technology Systems Security Risk Management		X																									
ICPG 500-1, Digital Identity												X													X	X	
ICPG 500-2, Attribute-based Authorization and Access Management												X			X								X	X	X	X	

	ANLVS	AUDIT	BASE-TDF	CDSM	CDSM-TDF	CSR-AUDIT	DHZM	DHZM-TDF	DHZMC-TDF	DOMEX	FAC-CES	FSD	IC-GENC	IC-ID	IC-SF	IC-TDF	IRM	ISM	ISM-ACES	ISM-Rollup	ISM-CAT-CES	MN-CES	ROLE-CES	RevRecall	UIAS	UIAS-APCS	USAGENCY-CES
ICS 500-13, Intelligence Community Optimized Network Email Display Name Format												X															
ICS 500-15, Intelligence Community Optimized Network Email Full Service Directory												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	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	X	X				X	
ICS 500-27, Collection and Sharing of Audit Data		X									X		X			X										X	
ICS 500-29, IC Digital Identifier												X												X	X		
ICS 500-30, Enterprise Authorization Attributes: Assignment, Authoritative Sources, and Use for Attribute-Based Access Control of Resources												X											X	X	X		
700 Series:																											
ICD 710, Classification and Control Markings System											X								X	X	X					X	
ICPG 710.1, Application of Dissemination Controls: Originator Control											X								X	X	X					X	
ICPG 710.2, Application of Dissemination Controls: Foreign Disclosure and Release Markings																			X	X	X						
ICS 700-2, Use of Audit Data for Insider Threat Detection		X																									
ICPG 704.5, Intelligence Community Security Database Scattered Castles																								X	X		
Memorandums:																											
OMB Memo - Enabling Mission Delivery through Improved Identity, Credential, and Access Management																								X			

UNCLASSIFIED

	ANLVS	AUDIT	BASE-TDF	CDSM	CDSM-TDF	CSR-AUDIT	DHZM	DHZM-TDF	DHZMC-TDF	DOMEX	FAC-CES	FSD	IC-GENC	IC-ID	IC-SF	IC-TDF	IRM	ISM	ISM-ACES	ISM-Rollup	ISM-CAT-CES	MN-CES	ROLE-CES	RevRecall	UIAS	UIAS-APCS	USAGENCY-CES
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	X	X			X	X	
IC CIO Memo - Improving Intelligence Community (IC) Identity, Credential, and Access Management (ICAM) to Achieve Greater Mission Effectiveness																		X	X	X	X	X	X		X	X	
DoD Issuances:																											
Department of Defense Directive Number 3300.03, DoD Document and Media Exploitation (DOMEX)										X																	
Department of Defense Instruction Number 5200.48, Controlled Unclassified Information (CUI)																		X									
Department of Defense Manual 5205.07, Special Access Program (SAP) Security Manual: Marking		X									X							X	X	X	X				X	X	
Department of Defense Instruction Number 8320.03, Unique Identification (UID) Standards for Supporting the DoD Information Enterprise														X													
Department of Defense Manual Number 5200.01, DoD Information Security Program (Vol 1-3)											X							X									
Federal Laws & Regulations:																											
Public Law 242-80th Congress													X														
Executive Orders:																											
Executive Order 13526 Classified National Security Information																		X	X	X							
Executive Order 13556 Controlled Unclassified Information																		X	X	X							
Executive Order 14028 Improving the Nation's Cybersecurity	X	X		X	X		X		X																		

UNCLASSIFIED

Presidential Directives																										
ANLYS	AUDIT	BASE-TDF	CDSM	CDSM-TDF	CSR-AUDIT	DH2M	DH2M-TDF	DH2MC-TDF	DOMEX	FAC-CES	FSD	IC-GENC	IC-ID	IC-SF	IC-TDF	IRM	ISM	ISM-ACES	ISM-Rollup	ISMCAT-CES	MN-CES	ROLE-CES	RevRecall	UIAS	UIAS-APCS	USAGENCY-CES
HSPD-12Homeland Security Presidential Directive 12: Policy for a Common Identification Standard for Federal Employees and Contractors																										
Implementing Directives:																										
32 CFR Parts 2001 and 2003Classified National Security Information; Final Rule																										
32 CFR Part 2002Controlled Unclassified; Final Rule																										
32 CFR Parts 2003The Interagency Security Classification Appeals Panel (ISCAP) Bylaws, Rules, and Appeal Procedures																										
32 CFR Parts 2004National Industrial Security Program Directive No. 1																										
ISOO Marking Booklet 2018Marking Classified National Security Information, Rev. 4 2018																										
CUI Category RegistryCUI Category Registry																										
CUI Limited Dissemination Controls RegistryCUI Limited Dissemination Controls Registry																										
CUI Marking HandbookCUI Marking Handbook																										
ISOO 32 CFR Part 2002 Clarification MemoISOO 32 CFR Part 2002 Clarification Memo, Date: June 4, 2019																										
IC CIO Directives:																										
Intelligence Community Markings System Register and Manual																										
Intelligence Community Public Key Infrastructure Certificate Policy																										