Attachment D – Adopted Industry Standards

SDO	Standard ID	Standard Title	Standard Description	Latest Revision/ Release Date[1]
APCO/TMA ANS (Formerly known as CSAA[2])	2.101.3-2021	*Alarm Monitoring Company to Emergency Communications Center (ECC) Computer-Aided Dispatch (CAD) Automated Secure Alarm Protocol (ASAP)*	Provides detailed information on data elements and structure standards for electronic transmission of new alarm events from an alarm monitoring company to an ECC.	Version 3.4 2021
APCO/ NENA ANS	1.102.3.2020	*Emergency Communications Center (ECC) Service Capability Criteria Rating Scale*	Assessment tool to evaluate current capabilities of the ECC against models representing the best level of preparedness, survivability, and sustainability amidst a wide range of natural and manmade events.	Version 3 January 30, 2020
ATIS/TIA	ATIS J-STD-110.01.V002	*Joint ATIS/TIA Native SMS to 9-1-1 Requirements and Architecture Specification*	Defines the requirements, architecture, and procedures for text messaging to 9-1-1 emergency services using native CMSP[3] SMS[4] or MMS[5] capabilities for the existing generation and next generation (NG9-1-1) PSAPs.	Release 2 May 1, 2015
ATIS	ATIS-0500017	*Considerations for an Emergency Services Next Generation Network (ES-NGN)*	Identifies standards and standards activities that are relevant to the evolution of emergency services networks in the context of next-generation telecommunications networks.	Version 1 June 2009
DOJ	CJISD-ITS-DOC-08140-5.9	*Criminal Justice Information Services (CJIS) Security Policy*	Provides information security requirements, guidelines, and agreements reflecting the will of law enforcement and criminal justice agencies for protecting the sources, transmission, storage, and generation of criminal justice information.	Version 5.9.1 October 1, 2022

[1] For any standards, if a newer version is available at the time of publication of this RFP, compliance will be judged relative to the latest version. The exception to this being NENA/APCO-INF-005.1-2014 for which compliance will be judged relative to NENA's updated Emergency Incident Data Object STA document

[2] Central Station Alarm Association

[3] Commercial mobile service providers

[4] Short message service

[5] Multimedia messaging service

IETF	RFC 3261	*SIP: Session Initiation Protocol*	Describes the SIP, an application-layer control (signaling) protocol for creating, modifying, and terminating sessions (including Internet telephone calls, multimedia distribution, and multimedia conferences) with one or more participants.	June 2002
IETF	RFC 6874	*Representing IPv6 Zone Identifiers in Address Literals and Uniform Resource Identifiers*	Extends RFC 3986 to include IPv6 to include zone identifiers and address literals.	February 2013
IETF	RFC 8865	*T.140 Real-Time Text Conversation over WebRTC Data Channels*	Specifies how a Web Real-Time Communication (WebRTC) data channel can be used as a transport mechanism for real-time text.	January 2021
NENA	REQ-001.1.2-2018	*NENA Next Generation 9-1-1 Public Safety Answering Point Requirements Document*	Provides requirements for functions and interfaces between an i3 PSAP and NGCS, and among functional elements associated with an i3 PSAP.	Version 1.1.2 June 10, 2018
NENA	STA-006..2-2022	*Standard for NG9-1-1 GIS Data Model*	Defines the GIS[6] data information, formats, requirements, and related information used in NENA Next Generation 9-1-1 (NG9-1-1) Core Services (NGCS).	September 23, 2022
NENA	STA-008.2-2014	*Registry System Standard*	Describes how registries (lists of values used in NG9-1-1 functional element standards) are created and maintained	Version 2 October 6, 2014
NENA	STA-010.3b-2021	*NENA i3 Standard for Next Generation 9-1-1*	Builds upon prior NENA publications including i3 requirements and architecture documents and provides additional detail on functional standards.	Version 3b October 7, 2021
NENA	INF-016.2-2018 (formerly 08-506)	*Emergency Services IP Network Design (ESIND) Information Document*	Provides information that will assist in developing the requirements for and/or designing an i3-compliant ESInet.	Version 2 April 5, 2018
NENA	08-751	*i3 Technical Requirements Document*	Provides requirements for ESInet architecture and security, among other i3 PSAP functions, and establishes a foundation for future i3 standards development.	Version 1 September 28, 2006
NENA/ APCO	54-750	*NENA/APCO Human Machine Interface & PSAP Display Requirements (ORD)*	Prescribes requirements for the human machine interface (HMI) display for the Next Generation 9-1-1 (NG9- 1-1) system.	Version 1 October 20, 2010

[6] Geographic information system

NENA	75-001 (Currently being updated; will become NENA-STA-040.2	*Security for Next-Generation 9-1-1 Standard (NG-SEC)*	Establishes the minimal guidelines and requirements for levels of security applicable to NG9-1-1 entities.	February 6, 2010
NENA	75-502	*Next Generation 9-1-1 Security (NG-SEC) Audit Checklist*	Provides the educated user a method to document an NG-SEC audit.	Version 1 December 14, 2011
NENA	INF-015.1-2016	*Next Generation 9-1-1 Security (NG-SEC) Information Document*	Provides mechanisms and best practices for cybersecurity for i3 systems.	Version 1 December 8, 2016
NENA	NENA-INF-040.2-2022	*Managing & Monitoring NG9-1-1 Information Document*	Provides guidance on best practices for monitoring and managing NG9-1-1 services and infrastructure.	Version 2 July 27, 2022
NENA	NENA-STA-021.1a-2022	*Standard for Emergency Incident Data Object (EIDO)*	Provides standard format for exchanging emergency incident data between disparate systems and agencies.	Version 1a April 19, 2022
NENA	NENA STA-031.1-2021	*Standard for Interconnecting Emergency Services IP Networks and Public Safety Broadband Networks*	Establishes standards for interconnections between ESInets and other broadband networks used by first responders.	October 14, 2021
NIOC[7]/ NENA	NIOC V1.0.0	*NIOC PSAP Credentialing Authority (PCA) Certification Validation Guidelines*	Provides the security requirements needed to support the secure validation for issuance of Certificates in NG9-1-1 by the PCA Certification Authorities (CAs) in the NG9-1-1 Public Key Infrastructure.	V1.0.0 February 9, 2022
NIST	FIPS[8] PUB 140-3	*Security Requirements for Cryptographic Modules*	Specifies security requirements that will be satisfied by a cryptographic module utilized with a security system protecting sensitive but unclassified information.	Version 2 March 22, 2019
NIST	Cybersecurity Framework	*Framework for Improving Critical Infrastructure Cybersecurity*	Provides standards, guidelines, and best practices that promote the protection of critical infrastructure.	Version 1.1 April 16, 2018

[7] NG9-1-1 Interoperability Oversight Commission
[8] Federal Information Processing Standards

TIA	TIA-942-B	*Telecommunications Infrastructure Standard for Data Centers*	Specifies the minimum requirements for telecommunications infrastructure of data centers and computer rooms, including single-tenant enterprise data centers and multi-tenant Internet-hosting data centers.	Revision B July 12, 2017