IJIS Institute

CAD-to-CAD Data Sharing
A Review of Recommended Standards

"A Plethora of Standards"

IJIS Institute

Public Safety Technical Standards Committee

February 2017

Principal Author
Becky Ward, FATPOT Technologies

ACKNOWLEDGEMENTS

The IJIS Institute would like to thank the following IJIS Institute Public Safety Technical Standards Committee (IPSTSC) contributors and their sponsoring companies for supporting the creation of this document:

Authors

Principal Author

Becky Ward, FATPOT Technologies

Principal Contributors

Mike Alagna, IJIS Institute
Chuck Brady, Zuercher Technologies LLC (See TriTech Software Systems)
Nate Daniels, Northrop Grumman Corporation
Rochelle Danielson, Versaterm
Tom Dewey, Advanced Justice Systems LLC
Steve Hoggard, Spillman Technologies (See Motorola Solutions)
Rick Meggison, Securus Technologies, Inc.
Charles Stortz, Logistic Systems, Inc.
Chris Rein, CSI Technology Group

Contributors

Bill Hobgood, City of Richmond, Virginia
Todd Maxwell, Booz Allen Hamilton
Kathy Wendt, SRA International, Inc. (See CSRA)

TABLE OF CONTENTS

INTRODUCTION

Quite often a Request for Proposal (RFP) is released for a Computer Aided Dispatch to Computer Aided Dispatch (CAD-to-CAD) interoperability platform that would share incident and unit status information with a number of Public Safety Answering Points (PSAPs.) These RFP's usually specify over a dozen standards with which the system provider must comply. Some of these standards are familiar in a CAD-to-CAD environment, but the inclusion of several are puzzling (see Section 1 in the End Notes.) Our research determined that more than half of the referenced standards did not directly apply to the CAD-to-CAD data exchange or had been supplanted by newer standards. Further research by IJIS Institute Public Safety Technical Standards Committee (IPSTSC) members found many other RFP examples that specified standards that were not applicable, as well as applicable standards that were missing.

What standards are applicable in a CAD-to-CAD RFP or RFP with CAD-to-CAD requirements? This paper begins a discussion of applicable standards but does not specifically address CAD standards or CAD functional requirements. This discussion will help to guide practitioners to include the most appropriate standards for CAD-to-CAD data sharing.

The information provided in this paper is important, as CAD-to-CAD system providers endeavor to remain current on standards development and adoption, but this task can be daunting. Conducting research on topics that are irrelevant or have been superseded distracts from a quality response, and can interject unnecessary and confusing information into a proposal.

Although potentially large in scope due to the sheer number of standards, this paper reviews seven (7) "standard requirements" requested in various RFPs, discusses the standard, and suggests if and how it applies to a CAD-to-CAD data exchange. This paper is intended to pave the way for follow-on papers, each addressing other standards pertinent to CAD-to-CAD data sharing.

Intended Audience

Readers of previous papers have asked for information about what standards are applicable in a CAD-to-CAD data exchange. This paper is a follow-on to the IJIS Institute Use Case in Public Safety CAD-to-CAD Data Sharing. Preceding white papers include *Change Management: Best Practices in Public Safety Data Sharing Projects* (provides guidance to practitioners on implementation planning for data sharing solutions); *Critical Decision Criteria for Data Sharing;* and

CAD-TO-CAD RFPS: TEST YOUR KNOWLEDGE ON STANDARDS. WHICH STANDARDS DO YOU THINK APPLY?

- NIEM
- HIPAA
- CJIS Security Policy
- EDXL
- N-DEx
- EIDD
- LEITS
- UICDS
- NENA ALI/GIS
- NG9-1-1
- CALEA
- NFIRS
- NEMSIS
- APCO/ANSI

Governance Agreements in Public Safety Information Sharing Projects. These white papers are recommended reading for anyone planning a data sharing project and can be found online at https://ijis.site-ym.com/?page=Reference_Papers.

Purpose

This paper provides background and assessment of a small number of "standards" found to be present in RFPs either focused on CAD-to-CAD or with a CAD-to-CAD component. Depending on the subject matter and goals of the RFP, certain standards are desirable or required. This paper takes a subset of the myriad of standards documented and discusses their relevance. Agency practitioners, service providers and consultants will be informed as to the applicability of the standard which will help clarify requirements in CAD-to-CAD RFPs. Readers of this paper should become aware that while there are standards available to choose from to insert into an RFP, practitioners and consultants should be thinking about the role of standards to achieve their CAD interoperability efforts as detailed in their RFP.

Methodology

IPSTSC members polled member CAD service providers, middleware providers, and agency practitioners to ascertain what standards had been specified in RFP's over the past two years. A matrix was compiled that captured:

- State of the agency that issued the RFP (examples: specific State or Federal Government)
- Primary applications specified in the RFP (examples: CAD-to-CAD, CAD, CAD and Records Management System (RMS), or CAD, RMS and Mobile, etc.)
- Was there a CAD-to-CAD component?
- What standards, if any, were mentioned in the RFP?

Section 2 in the End Notes is a compilation of all the standards mentioned in these various RFPs. The IPSTSC Committee determined that discussing all the standards requested would produce a paper hundreds of pages long, so a subset of the high-value standards was selected to present the research and conclusions by committee members.

EXECUTIVE SUMMARY

This paper suggests that many CAD-to-CAD RFP's or CAD-oriented RFP's that have requirements for CAD-to-CAD contain elements that are sometimes confusing, irrelevant or onerous. Regardless if this condition originates internally, from within the agency by writers of the RFP, or externally from contracted consultants, requiring adherence to a "smorgasbord of standards" may oppose the objectives of the RFP.

By examining a few of the standards found in various RFPs, we conclude that many are out of context and that the responding service providers often struggle to determine if there is a component of that standard that may be applicable of which they are unaware. Other requirements are clearly irrelevant to CAD-to-CAD data exchange in RFPs that do not have records transfer or reporting components. The more onerous requirements include those that require the service provider to agree to conformance with standards that have not yet been formulated and therefore have unknown level of effort and costs.

It is the opinion of this Committee that a better approach might be to ask RFP responders to discuss the standards to which they conform and why. Service providers might also be asked about their technology

roadmap as it pertains to standards. To better understand the topic, a general discussion of standards is provided as well as some background on technology and document standards.

STANDARDS OVERVIEW

What is a standard?

To many, this may seem an obvious and unnecessary question, yet the very existence of a document such as this white paper indicates that it's worthwhile to delve a bit more deeply. Although there are several definitions (some as a noun, some as an adjective), in practice there are some common terms or themes.

> "The nice things about standards is that there are so many of them to choose from."
> ~ Andrew S. Tanenbaum, American professor emeritus of computer science

Per OMB Circular A-119[1]: The term "standard," or "technical standard" includes the following:

- Common and repeated use of rules, conditions, guidelines or characteristics for products or related processes and production methods, and related management systems practices.
- The definition of terms; classification of components; delineation of procedures; specification of dimensions, materials, performance, designs or operations; measurement of quality and quantity in describing materials, processes, products, systems, services or practices; test methods and sampling procedures; or descriptions of fit and measurements of size or strength.

The International Organization for Standardization (ISO) defines a standard as—A document established by consensus and approved by a recognized body that provides for common and repeated use, rules, guidelines, or characteristics for activities or their results, aimed at the achievement of the optimum degree of order in a given context.[2] Furthermore, according to a standards review conducted by the National NG-911 Office[3]…"Standards can be *voluntary*—by themselves imposing no requirement regarding use—or *mandatory*. Generally, a mandatory standard is published as part of a code, rule, or regulation by a regulatory government body and imposes an obligation on specified parties to conform to it." Most standards are ***voluntary, consensus-based*** and ***open***:

- Voluntary—Use of standard is not mandated by law
- Consensus-based—Published standards have attained general agreement through cooperation and compromise in a process that is inclusive of all interested parties
- Open—Standards are not proprietary and are available for anyone to use

Types of Standards

There are numerous standards that are of interest and applicable:

- Product Standard—Most often are reflected in descriptions of hardware, software and other technology solutions
- Interface Standard—Requirements for connecting two or more systems, or technologies, to one another

[1] Section 3 of the Circular contains additional text description of what is a standard.
[2] Rules for the structure and drafting of International Standards. Available at: http://isotc.iso.org/livelink/livelink?func=ll&objId=4230456&objAction=browse&sort=subtype (last accessed February 26, 2015).
[3] https://www.911.gov/pdf/NG911-Standards-Identification-Analysis_03222016.pdf

- Data Standard—Definition, format, layout, characteristics of data stored within a system or shared across systems.
- Test Standard—Methodologies, processes, and other requirements associated with determining the performance of a product
- Performance Standard—Describes how a product or service should function
- Operational Standard—Operational standards could include standard operating procedures (SOPs), training guidelines and policies

In the Public Safety domain, two well-referenced standards bodies are the National Emergency Number Association (NENA) and the Association of Public-Safety Communications Officials (APCO). NENA is an organization whose mission it is to foster the technological advancement, availability, and implementation of a universal emergency telephone number system in the United States. APCO is the nation's oldest and largest organization of public safety communications professionals, with over 27,000 members, primarily consisting of state and local government employees who manage and operate public safety systems for law enforcement, fire, emergency medical and other public safety agencies. NENA and APCO are both Standards Development Organizations (SDO) accredited by the American National Standards Institute (ANSI). ANSI-Accredited Standards Developers offer processes that meet the Institute's requirements for:

- Openness
- Lack of dominance
- Balance
- Coordination and harmonization
- Notification of standards development
- Consideration of views and objections
- Consensus vote
- Appeals
- Written procedures

Why are Standards Important?

From the above discussion, standards derive from an approved body that:

- Establish a norm (and)
- Provide for common and repeated use (of)
- Rules, guidelines or characteristics (for)
- Products, processes or services

While compliance is not mandatory, non-adherence to relevant standards should give pause and generate questions. Public Safety standards are intended to help to provide better service to constituents, replicate best practices, lower costs in the long term, accelerate implementation and provide functional and operational benefits to practitioners. There should be a compelling reason if accepted standards from an approved, recognized and respected body are not embraced.

COMPLIANCE AND CONFORMANCE

There is a lot of discussion surrounding conformance versus compliance to standards. Standards come in play where consistency is required but has not been defined in regulatory language. The level that consistency can be mandated depends on what kind of compliance mechanisms exist. Practitioners should understand which standards have compliance mechanisms and only mandate "MUST comply" when compliance is possible, and they expect the provider to expend the resources and time needed to accomplish that. The most frequently misused requirement is that providers must be compliant with the National Information Exchange Model (NIEM.) NIEM is a framework that on its own does not enable any functionality and does not mandate compliance mechanisms for exchanges that are created using NIEM.

Conformance: In information technology, a state or acts of adherence to a certain specification, standard, or guideline. Sometimes used as a synonym for compliance. Conformance more often connotes a similarity to the model being followed within some allowed range. http://searchcio.techtarget.com/definition/conformance

Compliance: Compliance is either a state of being in accordance with established guidelines or specifications, or the process of becoming so. Software, for example, may be developed in compliance with specifications created by a standards body, and then deployed by user organizations in compliance with a vendor's licensing agreement. The definition of *compliance* can also encompass efforts to ensure that organizations are abiding by both industry regulations and government legislation.
http://searchdatamanagement.techtarget.com/definition/compliance

UNDERSTANDING XML AND JSON

XML and JSON Overview

First, let's briefly talk about document and technology standards. These document standards involve Standard Generalized Markup Language (SGML), Extensible Markup Language (XML) and JavaScript Object Notation (JSON). SGML to XML can be described as an evolution, whereas JSON is a revolution in that it is a "competitor" to XML. Document Standards are an evolution: starting first with Global Justice XML Data Model (GJXDM), then the National Information Exchange Model (NIEM) and then building upon NIEM with the Emergency Incident Data Document (EIDD).

XML, which superseded SGML, is a text file that you can open; computers open and read it as well. However, XML is "fat" with large file sizes. Computers take significantly longer to "read" XML files as it does not compress well to make it faster. Moreover, the same compression cannot be used with various types of data. Fast, effective compression must be employed if "real-time" data delivery is critical as is often the case with CAD-to-CAD data. Some CAD and middleware providers began looking for something faster and more efficient than XML for their mission critical applications.

Google uses JSON to overcome the problem of compression and speed for its browsers. Microsoft provides a good description of JSON and its benefits here: https://msdn.microsoft.com/en-us/library/bb299886.aspx. Note that the end result is the same, but since the file size is smaller, the data are delivered faster.

How It Applies to CAD-to-CAD

JSON provides an alternative to XML for CAD-to-CAD data exchange. The usage of JSON over XML can depend upon several factors, such as an agency's Enterprise Architecture, technical capabilities and/or a CAD provider's ability to support these exchange formats. XML is the most widely supported interchange format, and a CAD provider may not support JSON. In addition, all the Web Service tools natively support JSON because it's easier, faster and smaller. This results in a competitive and functional advantage to middleware and CAD service providers who embrace it.

The NIEM Technical Architecture Committee (NTAC)[4] is developing guidance that allows interested organizations to begin exploring JSON applications in the near term and provides an opportunity for feedback from the community based on actual experiences. The NIEM Program Office is currently developing guidance for using JSON-Linked Data (JSON-LD)[5], which recently gained acceptance as a World Wide Web Consortium (W3C) recommendation[6], in an Information Exchange Package (IEP). This guidance is applicable where the data to be exchanged is agreed upon before development.

From a CAD-to-CAD data exchange perspective, guidance or a standard is needed to define the rules of an exchange. If the rules are not defined, issues with exchanges will continue, such as a one-off of every exchange based on how the developer wants to do things.

Suggested CAD-to-CAD RFP Language

In a CAD-to-CAD RFP, the agencies should state the following information:

- The exchange format that each CAD provider can support
- The CAD-to-CAD exchange requirements or preferences

References

http://niem.github.io/technical/json/guidance/
https://en.wikipedia.org/wiki/JSON

UNDERSTANDING NIEM

NIEM Overview

NIEM was formed through a partnership agreement between the Chief Information Officers (CIO) of the U.S. Department of Justice (DOJ) and the U.S. Department of Homeland Security (DHS) in 2005. NIEM was originally targeted to leverage the data exchange standards efforts successfully implemented by DOJ's Global Justice Information Sharing Initiative (Global). NIEM extends the Global Justice XML Data Model (Global JXDM) to facilitate timely, secure information sharing across the whole of the justice, public safety,

[4] https://www.niem.gov/techhub/json
[5] http://json-ld.org/
[6] https://www.w3.org/blog/news/archives/3589

emergency and disaster management, intelligence, and homeland security enterprise. It has since grown to encompass an increasingly diverse set of information domains including Finance, International Trade, Immigration, etc.

NIEM provides a data model and structured approach to building and implementing data exchanges between different systems. Each data exchange stands on its own and is usually packaged as an Information Exchange Package Document (IEPD) or an Information Exchange Model (IEM). IEPD's can be created by anyone and are usually maintained by the content authors. It is up to the individual authors as to what level of support and compliance verification they choose to implement. Many IEPD's have been published online in the IEPD Clearinghouse and are publicly available.

How It Applies to CAD-to-CAD

NIEM applicability to CAD-to-CAD is currently evolving with the release of the Emergency Incident Data Document (EIDD) – see the EIDD section of this document. The EIDD provides a NIEM-based definition supporting the exchange of incident and unit data between CAD systems and other related public safety systems. Note that the EIDD will continue to evolve.

Suggested CAD-to-CAD RFP Language

The RFP should request CAD-to-CAD data exchanges using the EIDD format. If for some reason, EIDD cannot be used, the RFP should require the CAD-to-CAD exchange use the NIEM and conform to NIEM Naming and Design Rules (NDR) -- as it will decrease the future cost of migrating to the EIDD since many of the data structures can easily be reused. If exporting data to third parties, the exporting service shall produce XML documents using NIEM definitions, *e.g.*, N-DEx, SAR, etc., which is the national standard established by the Department of Homeland Security and the Department of Justice.

Note that if a new CAD-to-CAD interface is being funded by an Office of Justice Programs (OJP) grant, OJP requires the grantee to use the NIEM specifications and guidelines for that component of that grant. The Grantee must publish and make available without restriction all schemas (i.e., IEPD) generated, as a result of this grant, to the Clearinghouse as specified in the guidelines.

References

https://www.niem.gov/Pages/default.aspx
https://reference.niem.gov/
https://www.ise.gov/national-information-exchange-model-niem
https://en.wikipedia.org/wiki/National_Information_Exchange_Model
https://en.wikipedia.org/wiki/NIEM_conformance
https://it.ojp.gov/initiatives/niem
https://www.it.ojp.gov/niss
www.ncrnet.us

UNDERSTANDING THE EIDD

EIDD Overview

APCO International received approval from ANSI for an American National Standard (ANS) that identifies standard specifications for the exchange of emergency data. The EIDD provides standardized industry-neutral NIEM conformant (XML-based) specifications for exchanging emergency incident information to agencies and regions that implement next-generation 9-1-1 (NG 9-1-1) and IP-based emergency communications systems. Emergency incident information exchanges supported by the EIDD include exchanges between disparate providers' systems located within one or more public-safety agencies and with other incident stakeholders.

> "Data exchange is a core element of interoperability in a NG9-1-1 environment."
>
> ~APCO President Cheryl Greathouse

"Data exchange is a core element of interoperability in a NG9-1-1 environment," said Cheryl Greathouse, president of APCO International. "APCO is pleased to have worked with the National Emergency Number Association (NENA) to introduce this significant advance in data interoperability."

The IJIS Institute in concert with APCO is establishing a working group comprised of leading solution providers to review the specification for exchanging emergency incident information between agencies and regions that implement CAD and other next-generation emergency communications technologies. Emergency incident information exchanges supported by the new specification will encourage interoperability between different providers' systems located within one or more public safety agencies and with other incident information management stakeholders. The working group will unite technology users with industry solution providers in a collaborative environment to evaluate conformance specifications and validate testing methodologies to address real world challenges. IJIS will provide the Springboard™ conformance and certification platform and will work to encourage agency adoption of the specification during the acquisition process to foster broader adoption.

The EIDD and the IEPD including artifacts and schema have also been published. Lastly, NENA's Conveyance of the EIDD Working Group has been established to focus on developing an ANSI accredited NENA/APCO Standard for transporting (conveying) EIDDs between systems. The new Standard to be developed by this NENA/APCO working group will define how EIDDs are exchanged and transported from NG9-1-1 networks and systems.

The EIDD is intended to support a full complement of interoperable emergency incident data exchanges between a variety of public safety systems (CAD-to-CAD, CAD–to-RMS, CAD-to-mobile data, etc.). As with the implementation of any technical standard, the EIDD will have significant impact. It will foster data sharing, but it will also involve significant coordinated technical effort and an on-going commitment to the process. Initially, all the Public Safety technology solutions involved in the exchange of emergency incident information (*e.g.,* call handling, logging, dispatch, etc.) need to be modified to support EIDD transactions. External elements that exchange emergency incident information will also need to be modified to support EIDD transactions.

How It Applies to CAD-to-CAD

The intent of the EIDD document is to provide CAD providers with a standardized set of data that should be captured and available for CAD-to-CAD exchange, whether directly in a point-to-point interchange or an interchange through intelligent middleware. There are challenges ahead in implementing all the fields for both CAD and middleware providers. From the middleware provider perspective, there must be an ongoing, collaborative effort with the CAD providers. From the CAD provider standpoint, the most relevant question might be, "Is the market demand, across the spectrum of agency size and complexity, sufficient to make the cost of EIDD enhancements a good business decision?" Change can be costly, and there will be a price involved to implement EIDD-conformant CAD-to-CAD data exchange and other initiatives like NG9-1-1. From the practitioner perspective, agencies need to be convinced of the real value of the additional specifications and the costs that the early adopters are likely to pay.

Suggested CAD-to-CAD RFP Language

We are on the cusp of having an actionable standard for the automatic sharing of data in Public Safety. The conversation on how to implement the standard and how to assess its impact (the triple constraint of funding, quality and time) should be started soon. From the consultant perspective, what is the best advice to give their clients? Push for insertion of conformance to the EIDD in an RFP? Make conformance optional or mandatory? How will the benefits be articulated and justify the likely costs?

Until the full specification is released as a final standard, it will be difficult to hold service providers accountable for being "compliant." There will be a need for inspection and testing of standards-based interoperability specifications through a consensus-based process. Testing methodologies will need to unite technology users with industry solution providers in a collaborative environment to evaluate new interoperability specifications and validate the capability of standards-based solutions to address real world challenges.

References

https://www.apcointl.org/doc/911-resources/apco-standards/694-apco-nena-2-105-1-2017-ng9-1-1-emergency-incident-data-document-eidd/file.html
http://psc.apcointl.org/2017/02/02/ijis-emergency-incident-data-interoperability-working-group-call-for-expression-of-interest/
http://www.ijis.org/?page=Springboard
https://niem.gtri.gatech.edu/niemtools/iepdt/display/container.iepd?ref=CPnFNm8J4lA
http://www.nena.org/?JoinConveyEIDD_WG

UNDERSTANDING N-DEX

N-DEx Overview

The National Data Exchange (N-DEx) is one of the Criminal Justice Information Systems (CJIS) maintained by the Federal Bureau of Investigation (FBI.) The basic purpose of N-DEx is to share criminal justice information on a national scale and to provide the correct information to the appropriate people at the right time.

N-DEx is an incident-based information sharing system for law enforcement agencies, which securely collects and processes crime report data in support of investigations, crime analysis, law enforcement

administration, strategic/tactical operations, and national security. The N-DEx database contains data elements for incident reports, field interviews, arrest and citations, incarceration, booking, probation and parole.

Standard submission and query packages have been defined for N-DEx by the FBI, in addition to the on-line secure query capability. There are two submission packages conforming to the type of information being submit to N-DEx – one package is for incident and arrest and the other covers incarceration through parole submissions. The N-DEx submission packages are defined in the industry standard IEPD format. The submission and query packages can be found in the IEPD Clearinghouse. The N-DEx packages are NIEM conformant and based on the family of Law Enforcement Information Sharing Programs (LEISP) Exchange Standards (LEXS) IEPDs.

How It Applies to CAD-to-CAD

N-DEx is not an interface standard; it is a CJIS system. The N-DEx system is populated by submissions from law enforcement record management systems, including jails, courts and probation systems. In a CAD-to-CAD exchange environment, N-DEx submissions would not be utilized.

Suggested CAD-to-CAD RFP Language

None

References

https://www.fbi.gov/services/cjis/ndex
http://iepd.custhelp.com/
https://www.it.ojp.gov/niss

UNDERSTANDING HIPAA

HIPAA Overview

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) is United States legislation that provides data privacy and security provisions for safeguarding medical information. The Public Safety community is interested in HIPAA Title II, which establishes national standards for processing electronic health care transactions and requires health care organizations to implement secure electronic access to health data and to remain in compliance with privacy regulations set.

HIPAA Title II, sometimes called Administrative Simplification, has two primary areas of regulation. First is the standardization of certain electronic health care related transactions, and second is the implementation of controls to protect an individual's health information including a Privacy Rule and a Security Rule.

While there is no official HIPAA compliance certification program, the Department of Health and Human Services (HHS) has provided standards for the use and dissemination of health care information. These only apply to "covered entities" which include health plans, health care clearinghouses, and health care providers that transmit health care data. Providers that deliver software to support heath care providers are not "covered entities" while the agencies that use their software are the agencies to which these rules apply.

How it Applies to CAD-to-CAD

Although software providers are not "covered entities" as defined by HIPAA the two areas of Privacy and Security should be reviewed by providers to support their agencies compliance with HIPAA regulations. These providers supply Public Safety Software including CAD, RMS, Jail Management, Mobile Data, CAD-to-CAD, and CAD-to-RMS. While the Privacy Rule pertains to all Protected Health Information (PHI) including paper and electronic, the Security Rule deals specifically with Electronic Protected Health Information (EPHI).

Under Title II, the Security Rule directly addresses the means to safeguard PHI (Protected Health Information) against unauthorized uses or disclosures. Within that Security Rule, the Technical Safeguards section applies to policies, procedures and technology controls used to protect PHI contained within computer systems. There are five (5) standards listed in the Technical Safeguards section of the HIPAA that should be reviewed and include Access Control, Audit Controls, Integrity, Authentication and Transmission Security. Under Title II the Privacy Rule sets out requirements for contracts with business associates, use of authorizations, uses and disclosures of PHI, a notice of privacy practices and others.

In regards to a provider's responsibility in HIPAA compliance, their involvement depends on the system implementation. The agency or "covered entity" should ensure that the provider understands the rules regarding protected information. Access Control, Audit Controls, Integrity, Authentication and Transmission Security may be a part of a provider's solution and thus should be evaluated for compliance with the HIPAA standards.

Suggested CAD-to-CAD RFP Language

The provider(s) shall follow HIPAA Title II Security standards where applicable during the collection and/or use of Protected Health Information (PHI) resulting in the maintenance and use of both physical and electronic Protected Health Information (ePHI).

References

http://www.hhs.gov/
http://www.hipaajournal.com/hipaa-compliance-checklist/

UNDERSTANDING NG9-1-1

NG9-1-1 Overview

Before 1968, when emergency services were needed, the caller had to know the seven-digit number of the agency (police, fire or ambulance), they needed to provide the address of the emergency and the address of the wired phone they were using and they had to consider calling multiple agencies if they needed multiple services. Early Emergency Communications managers recognized that dialing a seven-digit string to reach emergency support was time-consuming and often resulted in errors.

In 1968 the current legacy 9-1-1 system got its start in Alabama. Callers could make one quick three-digit call and access the emergency services they required. Over time, with the advent of things like caller ID, the reporting and service dispatch process became more and more efficient. Today's legacy 9-1-1 systems have ANI (Automatic Number) ALI (Automatic Location) information and can reach out to many supporting

applications, processes and history files. What it lacks is the ability to accommodate the technology changes that have occurred over the last few decades (driven largely by mobile phones and social communication norms). That shortfall is what drives the NG9-1-1 initiative.

NG9-1-1 is often described as a change to the dispatch system that allows citizens to communicate using multiple media such as text, images and videos. While that is true, NG9-1-1 is much more than that. NG9-1-1 is the program that will transition emergency communications from a simple telephone call taking/dispatch function to a modern, more automated, and capable Emergency Communications Center.

The central tenant of NG9-1-1 is to move away from narrowband, circuit switched networks (that carry voice and only limited data today) and initiate an *Emergency Service IP Network* (ESInet). The ESInet employs an IP-based protocol that enables multi-media input to CAD, data sharing between Emergency Communications Centers and data availability for future enhancements. NG9-1-1, to be truly effective, must also function to a widely-adopted set of standards.

How It Applies to CAD-to-CAD

CAD-to-CAD communication (as well as CAD-to-anything communication) can be accomplished through the implementation of the EIDD standards discussed earlier in this paper, coupled with the NENA i3 Standards and the other "back office" NG9-1-1 artifacts. The reality, however, is that most CAD service providers will not implement EIDD unless it is apparent that the industry is moving in that direction. Another path would be for industry to build a middleware device that will implement and manage EIDD machinations such that the CAD provider only has to interface to the middleware. That approach makes the cost more predictable, the project more manageable and the implementation faster.

Suggested CAD-to-CAD RFP Language

The RFP must define the end state desired. It must detail the agencies expectation and provide action verbs such that the response is measurable. The following are some considerations when developing an RFP but are provided as an example only and are not all inclusive.

- Equipment shall be compliant with NENA i3 standards.
- All Dispatch Software must employ EIDD standards for communication outside the CAD suite.
- The CAD system must interface to call-input services using Internet Protocol (IP).
- Provider shall describe their plan to migrate existing NG9-1-1 services to the ESInet including processes and procedures for interconnection.

NG9-1-1 provides a multitude of means of contacting the PSAP. Call-takers must be capable receiving calls through any of the following means: Text messaging, photos, videos or other digital information. The NG9-1-1 communications received and stored in the CAD call history must be identifiable and transferable to any partner in the CAD-to-CAD configuration. The potential volume of data that NG9-1-1 can send to a Public Safety Answering Point (PSAP) and stored in a CAD call history is quite large. The provider must explain how the NG9-1-1 data in the CAD call history will be treated and handled by the CAD-to-CAD transfer and/or middleware.

References

http://www.nena.org/?NG9-1-1_Baseline
http://www.sustainabledevelopmentmagazine.com/?p=1405
http://www.911.gov/pdf/NG9-1-1-StandardsIdentificationAnalysis-jan2014.pdf

See also:
"Detailed Functional and Interface Standards for the NENA i3 Solution." The National Emergency Number Association (www.NENA.org)
"Next Generation 911 (NG9-1-1) Standards Identification and Review." The National 911 Program Office (www.911.gov)
"FirstNet Statement of Objectives Document." First Responder Network Authority (www.FirstNet.gov)

UNDERSTANDING CJIS SECURITY POLICY

CJIS Security Policy Overview

The Criminal Justice Information Services (CJIS) Security Policy provides a minimum set of security requirements for access to the FBI's Criminal Justice Information Services (CJIS) Division systems and information and to protect and safeguard Criminal Justice Information (CJI). CJI is defined as the data that FBI CJIS houses for various purposes to support the mission of law enforcement and other civil agencies.

Through a combination of requirements, guidelines and agreements with other agencies, the goal of the CJIS Security Policy is to protect the CJI data from the time it is created until it is released to the public via authorized dissemination such as within a court system. According to the policy, data are to be protected whether at rest or in motion from unauthorized access. The CJIS Security Policy has been augmented by many states to extend and clarify the policy in regards to using various technologies, hosting and accessing environments.

How It Applies to CAD-to-CAD

First, in the CAD-to-CAD environment, this paper does not envision one CAD system accessing CJIS, that is making CJIS, state or local criminal justice inquiries, through a partnering CAD system. This paper further assumes that each CAD system, in the partnering CAD-to-CAD configuration, is already, itself, CJIS Security compliant. During CAD operations, CJI data may be copied, pasted and/or attached as part of the incident/call history and incident information. If CJI information attached to an incident is transferred to a partnering CAD system, the transfer must meet/comply with CJIS Security Policy.

In addition, to the encryption of the communications path, CAD-to-CAD middleware products must assume the presence of CJI data in incident data and apply appropriate CJIS Security Policy for the storage and tracking of the incident data for the longevity of the incident within middleware environment. If a CAD-to-CAD middleware is not being used, the assumption (*e.g.,* exchange policy) is that the receiving CAD entity will handle CJIS CJI marked data in accordance with the CJIS policy. When dealing with a non-law enforcement CAD system, such as a Department of Transportation (DOT) system, CJI data, such as personal information, needs to be identified in the incident history, such that the CAD-to-CAD middleware/interface can appropriately redact the CJI information. The CAD-to-CAD governance agreement must cover what type of CAD incidents and information can be transferred to non-Law Enforcement systems. If there is no use of FBI CJIS data within the system, then the CJIS Security Policy would not apply.

Suggested CAD-to-CAD RFP Language

The RFP must define the end state desired for CJIS compliance. The following are some considerations when developing an RFP but are provided as an example only and are not all inclusive.

- The Provider shall comply with all Criminal Justice Information Services (CJIS) security policies where applicable during the collection and/or use of information as it anyway relates to CJIS.
- The CAD-to-CAD environment must be fully CJIS compliant.
- The CAD-to-CAD communications must be fully encrypted end-to-end and function in a shared network environment and provide CJIS compliance.
- The CAD-to-CAD middleware must provide continuity and comply with CJIS security for storage of the CAD call history.
- If a non-Law Enforcement system requires access to CAD call histories then, the CAD-to-CAD middleware must redact and encrypted the CAD call information to be CJIS compliant.
- If the CAD-to-CAD middleware provides remote access, *e.g.*, web or in-vehicle, into the application. The remote access must comply with CJIS Security Policy standards.

References

https://www.fbi.gov/file-repository/cjis-security-policy-v5_5_20160601-2-1.pdf

CONCLUSION

This paper chose seven (7) standards and discussed their relevance to CAD-to-CAD RFP language. It is this Committee's intent to tackle additional standards in subsequent papers to help educate the industry and influence the development of better RFP requirements. Practitioners should understand the relevant standards and be careful about over-specifying what standards are important to their project. Consultants need to understand that shot-gunning a plethora of standards into an RFP injects distraction into the response and may elevate the cost of the solution. The result may either inflate prices through assumption of inferred scope or cause qualified providers to withdraw due to an impression they would be noncompliant.

Both CAD providers and consultants need to understand the boundaries of CAD functionality and performance versus CAD-to-CAD functionality and operations. While some of the stated requirements may apply to CAD and its intended operation in its holistic environment, in a CAD-to-CAD RFP these same requirements may not apply. Practitioners may well be better served by asking service providers to discuss their adherence to standards, why they do so, and their technology and business roadmap for doing so in the future. A narrative approach is likely to reveal much more about the provider and its technology.

END NOTES AND REFERENCES

Section 1

The following are requirements taken from the CAD-to-CAD RFP published in 2015. *Note that misspelling and errors were copied from the document and are not, herein, typographical errors.* Note that the IPSTSC Committee is providing them for reference and is NOT recommending them for including into a CAD-to-CAD RFP in their current format.

HIPAA

- HIPAA Compliance http://www.hhs.gov/
  - Describe the proposed CAD-to-CAD solution's ability to meet HIPAA standards.
- Under Services Solicited section:
  - The Offeror will be responsible for the following project components:
    - Researching requirements and proper protocol concerning the collection of CAD information and must comply with Health Insurance Portability and Accountability Act ("HIPAA"), Criminal Justice Information Services (CJIS), National Information Exchange Model (NIEM), and other applicable public safety information and data requirements.
- Under the Technical Specifications section:
  - The federal government has taken the lead in developing standards for facilitating information sharing among local, state and federal first responders and emergency operations managers. The proposed CAD-to-CAD solution shall adhere to these standards.

NIEM

- National Information Exchange Model (NIEM) http://www.niem.gov/
  - Describe compliance with NIEM standards. List all specifications, functionality and features related to proposed CAD-to-CAD version.
  - Describe any completed and existing projects implementing NIEM standards relevant to proposed CAD-to-CAD version. Provide public safety customers point of contact information (if applicable).
  - Describe current plans, processes and functionality related to N-DEX standards.
  - Describe current plans to comply with proposed Emergency Incident Data Document (EIDD) and Incident Data Exchange (IDE) requirements.

N-DEx

- Describe any completed and existing projects implementing N-DEX standards relevant to proposed CAD-to-CAD system. Provide public safety customers point of contact information (if applicable).
  - Identify criminal justice entities that the company is a participant related to the development and implementation of NIEM and N-DEX standards.

LEITSC

- Law Enforcement Information Technology Standards (LEITS) https://it.ojp.gov/documents/LEITSC_Law_Enforcement_CAD_Systems.pdf
  - Describe the proposed CAD-to-CAD solution's ability to meet LEITS standards.

NFPA

- National Fire Protection Association (NFPA) http://www.nfpa.org
  - Describe the proposed CAD-to-CAD solution's ability to meet NFPA standards.

UICDS

- Unified Incident Command and Decision Support (UICDS) https://www.napsgfoundation.org/wp-content/uploads/2014/04/UICDS-Introduction-for-Geospatial-Technology-Workshop-4-17-14.pdf
    - Describe the proposed CAD-to-CAD solution's ability to meet UICDS standards.

CJIS Security Policy

- FBI Criminal Justice Information System (CJIS) Security Policy https://www.fbi.gov/services/cjis/cjis-security-policy-resource-center
    - Describe the proposed CAD-to-CAD solution's ability to meet CJIS 5.1 or latest standards and the California Law Enforcement Telecommunications System (CLETS) requirements.

NENA ALI/GIS

- National Emergency Number Association (NENA) ALI/GIS Standards http://www.nena.org/?page=DataFormats
    - Describe the proposed CAD-to-CAD solution's ability to meet "NENA Recommended Formats and Protocols for ALI Data Exchange, ALI Response and GIS Mapping," NENA 02-010 of January 2002 as a minimal standard. All GIS/Mapping solutions shall comply with the NENA formats and standards.

NG9-1-1

- Next Generation 9-1-1 (NG-9-1-1) http://www.its.dot.gov/ng911/
    - Describe the Offeror's involvement with the development of NG-9-1-1 standards and how NG-9-1-1 will impact the proposed CAD-to-CAD system's functionality and features.
    - Describe any NG-9-1-1 capabilities, functionality, and features of the proposed CAD-to-CAD system.
    - Describe how the company will update existing CAD-to-CAD systems as new NG-9-1-1 standards, functionalities, and features are developed.

CALEA

- Commission on Accreditation for Law Enforcement Agencies (CALEA) http://www.calea.org/
    - Describe the proposed CAD-to-CAD solution's ability to meet or comply with CALEA standards.

NFIRS

- National Fire Incident Reporting System (NFIRS) http://nfirs.fema.gov/
    - Describe the proposed CAD-to-CAD solution's ability to meet NFIRS standards.

NEMSIS

- National EMS Information System (NEMSIS) http://nemsis.org/
    - Describe the proposed CAD-to-CAD solution's ability to meet NEMSIS V2 Gold standards.

APCO

- APCO / ANSI http://www.apcointl.org/standards/apco-standards-for- download.html
    - Describe the proposed CAD-to-CAD solution's ability to meet ANSI standards for Common Incident Codes for Data Exchange

OTHER

- "The federal government and other parties such as APCO and NENA occasionally update and improve the above-referenced standards or develop new ones. In that the City may desire to adopt such future standards, it is mandatory that the CAD-to-CAD Offeror will monitor these developments and upgrade its offerings as necessary to comply. As the time between purchase of a CAD-to-CAD system and their implementation may be significant, it is possible that updated

standards would have been released in the interim. LA City will not accept products that will be outdated by the time they are installed. The Offeror shall describe the proposed CAD-to-CAD solution's ability to meet this standard."

Section 2

The following are standards that were taken from various RFP's researched by members of the IJIS IPSTSC Committee specifically requesting CAD-to-CAD or having a CAD-to-CAD component:

- 29 U.S.C.794d
- 36 CFR 1194 Section 508
- APCO Software Development standards
- APCO/ANSI
- APCO/IJIS UCAD FR
- APCO-25
- CALEA
- CJIS
- CJIS Security Policy
- EDXL
- EIDD
- FIPS
- Global Justice XML
- I3
- IAD
- IDE
- JRA
- LEITS
- LEITSC
- NCIC
- N-DEx
- NEMSIS
- NENA ALI/GIS
- NENA NG911
- NFIRS
- NFPA 1221, 1061, 1710
- NG911
- NIBRS
- NIEM
- NIMS
- NIST
- NMEA
- OSHA
- PMI
- State Public Records Law
- TAIP
- US DOT
- "All applicable federal, state and local health, environmental and safety laws, regulations, standards, codes and ordinances, regardless of whether or not they are referred to by the City."
- "Applicable state and federal security standards."
- "…must comply with Health Insurance Portability and Accountability Act ("HIPAA"), Criminal Justice Information Services (CJIS), National Information Exchange Model (NIEM), and other applicable public safety information and data requirements."
- "The federal government has taken the lead in developing standards for facilitating information sharing among local, state and federal first responders and emergency operations managers. The proposed CAD-to-CAD solution shall adhere to these standards."

ABOUT THE IJIS INSTITUTE

The IJIS Institute unites the private and public sectors to improve mission-critical information sharing and safeguarding for those who protect and serve our communities. The IJIS Institute provides training, technical assistance, national scope issue management, and program management services to help government fully realize the power of information sharing.

Founded in 2001 as a 501(c)(3) nonprofit corporation with national headquarters on The George Washington University Virginia Science and Technology Campus in Ashburn, Virginia, the IJIS Institute has grown to over 400 member companies and individual associates from government, nonprofit, and educational institutions from across the United States.

The IJIS Institute thanks the IJIS Public Safety Technology Standards Committee for their work on this document. The IJIS Institute also thanks the many companies who have joined as Members that contribute to the work of the Institute and share in the commitment to improving justice, public safety and homeland security information sharing.

For more information on the IJIS Institute:

- Visit the website at: http://www.ijis.org/,
- Follow the IJIS Institute on Twitter: @ijisinstitute,
- Read the IJIS Factor Blog; and
- Join us on LinkedIn at: Justice and Public Safety Information Sharing and IJIS Institute.

About the IJIS Public Safety Technology Standards Committee

The purpose of the IJIS Public Safety Technology Standards Committee is to promote and contribute to the development of technical and functional standards for public safety information technology components, to provide industry input and policy review on technical matters faced by the public safety community, and to oversee IJIS Institute projects assigned to the Committee.