Table of Contents

The answers shown here are based on the point in time when they were provided, based on the then current applicable specifications. All answers are subject to change if the applicable specifications change. NENA will endeavor to keep this document in sync with any changes made in the applicable specifications that would cause these answers to be outdated. Those applicable specifications (Standards) are the normative source, and this document is informative.

Table 1: Q&A about what an Emergency Incident Data Document (EIDD) is and is not.		
EIDD FAQ #	**Questions**	**Answers**
1.	What is an EIDD?	"**EIDD**" is an abbreviation for **E**mergency **I**ncident **D**ata **D**ocument. A National Information Exchange Model (NIEM) conformant, object that is used to share emergency incident information between and among authorized entities and systems. The EIDD represents the state of an incident as known by the sender at the time it was sent. The EIDD and its conveyance mechanisms replace the serial port data connection between CPE and CAD, as well as providing a standardized CAD to CAD interface. It standardizes incident status update mechanism, between responders and agencies, between agencies working multi-agency incidents, and also provides a standardized way to send incident data to EOCs, tow truck operators, utilities and even news organizations.

Table 1: Q&A about what an Emergency Incident Data Document (EIDD) is and is not.			
2.		Why do we need EIDDs?	We need a way for one system or agency that has information about an incident to send that information to another system or agency using a standard format. That way, both systems can understand the information, even if the systems are from different vendors or operated by different agencies. In NENA documentation, these systems are often also called functional elements (FE).
3.		Where are the specifications for the EIDD?	**There are several documents where the specifications and requirements relating to EIDDs are published:** • **The format and XML schema for EIDDs** is specified in an APCO/NENA standard that can be downloaded: NENA/APCO Emergency Incident Data Document (EIDD) • **The requirements for PSAP functional elements for sending and receiving EIDDs** are included in the NENA/APCO NG9-1-1 PSAP Requirements Document Standards that detail EIDD specifications that are under development in NENA's Agency Systems Committee. • **EIDDs used for transferred calls and other aspects of EIDDs** are published in NENA-STA-010 Detailed Functional and Interface Standards for the NENA i3 Solution **NENA Working Groups are currently developing additional documentation on EIDDs:** • **EIDD Conveyance:** Conveyance of Emergency Incident Data Document (EIDD) Working Group • **EIDD Management:** Management of Emergency Incident Data Documents (EIDD) **IDX Functional Element:** i3 Architecture
4.		What kind of information is in an EIDD?	An EIDD contains information about a single incident including: the calls related to that incident, the responders assigned to the incident, the participants and vehicles involved in the incident, etc. EIDDs will often include the caller's information like name, number, and location. EIDDs can also include agents' notes, information about responder equipment, agencies involved in the incident, and lots of other incident information. You can find details on all of the kinds of information that can be transferred in an EIDD in the NENA/APCO Emergency Incident Data Document (EIDD). There is also a handy Excel spreadsheet guide to all of the kinds of XML elements that there can be in an EIDD in the EIDD Mapping Spreadsheet.
5.		Is there a standard XML schema for the EIDD?	Yes. The NIEM-Conformant IEPD (Information Exchange Package Document) is available here: NIEM IEPD (Schemas & other documents)

Table 1: Q&A about what an Emergency Incident Data Document (EIDD) is and is not.		
6.	What is the relationship between an incident record and EIDD?	An incident record is an internal representation of the incident information and is typically proprietary to an agency's system. An EIDD is an external representation of the current state of an incident as known by the sending FE.
7.	Does the user have to push a "send EIDD" button to send EIDDs to other systems?	No – the system sends EIDDs to other systems when the Incident state changes, whether because a user entered something, or because the system received automated data like the location of an assigned unit. For user-entered information, there may be a "save" or "commit change" button, but it's really the fact that the Incident state has changed that triggers EIDDs being sent, rather than the button push.
8.	How are EIDDs generated?	An EIDD is a data object, an XML data object specifically. EIDDs are generated by software in response to changes in incident status. Some EIDDs may be generated as a result of human action like choosing a responder in a dispatch ("CAD") system. Some may be generated automatically, like a change in a responding vehicle's location determined by an AVL system. EIDDs will not be displayed to users directly. Some user interface may (or may not) change in response to receipt of an EIDD, but that depends on the function of the user interface and its implementation. EIDDs are computer to computer notifications of incident state, as known by the sender, at the time it was sent. They are standardized to allow call ("CPE") to dispatch ("CAD"), CAD to CAD, CAD-to-responder (e.g MDT), PSAP to EOC, or any other systems from multiple vendors to interoperate where incident state is exchanged.
9.	Is an EIDD a complete record of the call, or something less?	No, an EIDD represents the state of an **Incident**, which may have zero or more **Calls** associated with it. An EIDD also represents the state of an incident **at the time it was sent**, as known by the system or agency that sent it. (See EIDD FAQ# 10)
10.	If an EIDD is not a complete record of the call, how does that look?	An EIDD only includes INCIDENT (not just "call") information as known by the FE that is generating the EIDD at the time it was sent. If there is a change in the state of an incident, that change is included in a new EIDD. The EIDD has no incident history.
11.	Is an EIDD only a snapshot in time that carries data from one point to another?	Yes.

		Table 1: Q&A about what an Emergency Incident Data Document (EIDD) is and is not.
12.	Does the EIDD accumulate the entire data exchange record?	No. The accumulation of the entire data exchange record for an Agency is located in the Agency's logger(s).
13.	How does an FE or Agency get an EIDD?	The EIDD Conveyance working group is writing standards that define how EIDDs are sent ("conveyed"). Current draft text provides several mechanisms including a "push" mechanism where the FE that creates the EIDD sends it to some other FE without any prior action by the recipient. This is used in, for example, a typical dispatch operation, where the sending FE (for example, the Call Handling FE) sends an EIDD to, for example, a Dispatch FE, to request dispatch. The sender includes in the EIDD what it knows about the incident and the recipient does whatever it believes is appropriate for that incident. There is also a proposed "pull" operation where the receiver asks (in advance) with a subscription mechanism to receive EIDDs based on a "filter" specification. The subscription mechanism is typically used to get periodic updates of incident state as an incident progresses. It can also be used to inform an agency of new incidents opened by the sender that match a set of criteria specified in the subscription.
14.	If an EIDD is only a snapshot in time, where are the EIDD transactions logged?	EIDDs must be logged when they are sent. To get history, you query the logger of the sender. EIDDs may be logged by the recipient. If they are, you can get history from the recipient's logger, but the sender's logger is "authoritative".
15.	Does an EIDD have a complete history of the incident at the time it is first generated and then only updates after that?	An EIDD represents the state of an incident as known by the sender at the time the EIDD was sent. The EIDD is a snapshot in time, not a complete history. If the recipient uses the subscription mechanism, then whenever the state changes sufficiently, the sender will create a new EIDD and send it. That updates the incident at the recipient. At present, the draft conveyance text expects each EIDD to contain the entire state of the incident as known by the sender, and not changes to the state. If the recipient needs to know what happened before an EIDD was sent, they get it from the logger. If they need to know the state after an EIDD was sent, they subscribe to the incident at the sender, and they will get new EIDDs when state changes.

		Table 1: Q&A about what an Emergency Incident Data Document (EIDD) is and is not.
16.	Other i3 data items can be sent "by value" or "by reference". What does EIDD transmission use?	The current draft conveyance offers both in some circumstances. Most transmission is "by value", but an FE can create a URI which, when dereferenced, would return the current EIDD (value). Similarly, an FE can create a URI which is used with the subscription service to receive EIDDs. The subscription URI is another form of EIDD by reference.
17.	How is a Reference obtained?	A reference may be obtained from a transferred call in the SIP signaling. The "Service and Agency Locator" can return a URL for an agency 's "EIDD reference factory" service, which, when queried with an incident ID, returns a URL that can be used with the dereference service. As above, the FE can also create a subscription URI which also is a form of EIDD by reference.
18.	How do I control what EIDD information is made available?	As with all i3 services, the content of the EIDD, the subscription service, the dereference service and the reference factory service responses are all subject to the agency's Data Rights Management policy, and thus the EIDD owner determines who can use these services and what data they can obtain from these services.
19.	When an EIDD payload is done by-reference, how does that look?	An FE can generate a URI and distribute the URI. An FE in possession of the URI "dereferences" it by using an HTTP Get operation, which access's a dereference service, which returns the then-current value of the EIDD. If the GET is repeated later, a new EIDD with current state is returned.
20.	When does an EIDD get generated from triggered events (e.g., note-taking?	In general, any event which would change the state of an incident sufficiently such that at least one field of the EIDD would change is sufficient to generate a new EIDD. However, with the subscription service, the recipient can specify content, rate and/or location filter criteria that affects when it receives EIDDs. All filters can reduce the number of EIDDs sent, but the rate filter also has a minimum rate specification, which if used can cause an EIDD to be sent even when no value changes.

Table 1: Q&A about what an Emergency Incident Data Document (EIDD) is and is not.		
21.	Does the EIDD calltaker note data component, or any other data component that contains multi-line text get generated after a single character is typed, and after every character is typed, or only when the creator 'saves' or otherwise causes the entry to be captured into an EIDD?	The current proposed transport draft uses Subscribe/Notify to send updated EIDDs. The mechanism includes filters that allow the recipient to control the rate of transmission. The sender can decide how often to send updates, which could be as often as every character, or as little as complete notes. The recipient can limit how often it receives EIDDs using the rate filters.
22.	The APCO-NENA EIDD document says that an EIDD does not provide historical data. What does that mean?	It means that you only get the entire (not delta) CURRENT 'state' of the incident, as known by the sender. Historical data is stored in, and retrieved from the logging service.
23.	How do I determine that something has changed during the course of an incident?	At least one field will be different from the previous EIDD received for this incident, but see below*. The EIDD itself doesn't indicate that something changed. The UI determines what the agent/user becomes aware of, and how they are notified. * The conveyance document describes the use of "rate" filters, one of which is a minimum rate. An EIDD may be sent to achieve the minimum rate, which may not have any fields different from the prior EIDD.

Table 1: Q&A about what an Emergency Incident Data Document (EIDD) is and is not.

24.	Where do EIDD data files get stored?	They don't get stored. There is no such thing as a "EIDD data file". EIDDs sent are logged, so there is a copy in the logging service of the sender. Received EIDDs may be logged, so there may be a copy in the logging service of the recipient. Anything else is implementation dependent. Systems that exchange EIDDs probably store the information in their own incident record. Neither the EIDD standard nor STA-010 define how the data in EIDD messages must be physically stored in FEs that exchange EIDD messages.
25.	Is there a way to show the recipient that current data within the EIDD is not the original data (e.g., location data was updated/changed – is there indication of this to the PSAP)?	No, but the history is in the logging service.
26.	When is a new EIDD sent?	An EIDD is sent when a significant change in incident state changes. At minimum, at least one data component in the EIDD has to change from the prior EIDD sent for this incident. Also see EIDD FAQ# 20, and EIDD FAQ# 23. Policy in the sender may restrict sending an EIDD when there are what it considers minor values that ARE visible in a data component. The usual example is location of a responding unit.
27.	Is it going to create a trail for us follow?	The "trail" is in the logger.

	Table 1: Q&A about what an Emergency Incident Data Document (EIDD) is and is not.	
28.	Does it create a map?	EIDDs don't create a map. Information in the EIDD can be used by the User Interface to create or update a display that may include a map.
29.	Will actions such as rebid create another EIDD?	"Rebid" would create a new EIDD if and only if the response changes by some policy determined value AND the filter for the recipient requests it.
30.	What is the difference between an EIDD vs Incident Record	"Incident Record" is not standardized, EIDD is. An implementation may have more data (non-standardized) in its local incident record than in an EIDD. (Also see EIDD FAQ# 6)
31.	What notes are updated?	There is a data component in an EIDD that is called a note, and there are references to notes in several other data components. You can "update" any note, just like you can "update" any other data component. You send an EIDD that has a change in that data component.
32.	Which PSAP workflows will generate an EIDD?	EIDDs are sent when a new incident is generated (either receipt of call or a self-declared incident), and whenever state changes. State changes are determined by the EIDD data components: when any of those data components has at least one element that changes, the agency that determines the changes sends EIDDs. Events that might cause an EIDD to be sent include (not limited to): • Call Handling (call received, answered, transferred, terminated) • Dispatch operations (request another agency dispatch, or select a unit to dispatch) • Incident classification • Responder unit reports (arrived on scene, determination of victim/perpetrator/witnesses, • Clearing operations

	Table 1: Q&A about what an Emergency Incident Data Document (EIDD) is and is not.	
33.	How is access to the information in an EIDD controlled?	Standard NG9-1-1 Data Rights Management mechanisms apply to EIDDs. There are restrictions on what data may be passed to an agency that the sender received from another agency. Data rights management for data received from another agency requires additional development work. In the meantime, a way to control access to 3rd parties is to give a link to the data, rather than the data itself (by ref versus by value).
34.	How are new values for the 'Reason for Issue' field in the EIDD generated?	Reason for Issue values are defined in a Registry managed by the NENA Registry System, located at: http://technet.nena.org/nrs/registry/EIDD-ReasonForIssue.xml. Creating a new value requires a specification document and expert review.
35.	An EIDD contains Current State. What does Current State always include?	Current state, as known by the entity sending the data at the time the EIDD was sent, will include the data components that the sender is aware of, which may differ at any point in time. However, several elements are always included in an EIDD. Those are listed as 'mandatory' elements in the EIDD header, as shown in the APCO-NENA EIDD Standard, found at: http://www.nena.org/?EIDD.

Table 2: Q&A about what the Incident Data Exchange (IDX) is and is not.

IDX FAQ#	Questions	Answers
1.	What is the purpose of an IDX?	An Incident Data Exchange (IDX) is a functional element that aggregates EIDD information from multiple FEs within an agency and creates a composite EIDD that represents the entire state of an incident as known by the agency at the time the aggregated EIDD was sent by the IDX. To accomplish this task, the IDX receives EIDDs from all the constituent FEs within the agency and combines them using an algorithm to create a single composite EIDD. FEs or agencies inside or outside the agency can then obtain the composite EIDD from the IDX. There is a second type of IDX that coalesces information from more than one IDX for a multi-agency incident. It is called the Inter-agency IDX. The Inter-agency IDX obtains EIDDs from all the agencies involved in an incident and creates a composite view of the incident from the constituent EIDDs. Any (authorized) agency can then get a unified view of the incident by obtaining an EIDD from the Inter-agency IDX.
2.	Where are the specifications for the IDX?	They will be in V4 of STA-010, but work has not yet begun on the IDX section.
3.	From an operational perspective how does the IDX get EIDDs	The IDX subscribes to all the FEs within an agency and obtains updates for every incident from every FE within the agency.
4.	Can the IDX send EIDDs by reference?	The IDX may deliver coalesced EIDDs by reference. If it does so, then it does the dereferencing for those references.

Table 2: Q&A about what the Incident Data Exchange (IDX) is and is not.

5.	Is the IDX capable of receiving a constituent EIDD 'by reference'?	No. The IDX always subscribes to the FEs that supply it constituent EIDDs, therefore the EIDDs are sent by the FEs, to the IDX 'by value'.
6.	If an EIDD is received by an IDX containing data 'by reference', what is in the coalesced EIDD it sends?	If the data was received 'by reference', it is sent 'by reference'. If the data was received 'by value', it is sent 'by value'.
7.	When an outside organization wants to obtain an EIDD, does it do it through the IDX?	In most cases yes. Policy can determine if an FE in an outside organization is permitted to obtain EIDDs from FEs other than the IDX.
8.	How does an FE locate the IDX?	The agency locator (defined in STA-010) will contain the address (URI) of the IDX that needs to be interrogated about incident information for an agency.

		Table 2: Q&A about what the Incident Data Exchange (IDX) is and is not.
9.	Does the IDX always "mediate" requests for an EIDD? Where mediate means that all requests for EIDDs go through an IDX.	Within an agency, one FE may send/receive EIDDs to other FEs directly. For FEs outside the agency, see FAQ <insert the FAQ above> While it is not mandatory that FEs within an agency use the IDX, there are situations and functions that benefit from having the IDX do mediation. In particular, the coalescing algorithm used by the IDX is complex, and should not be duplicated in other FEs.
10.	Can EIDDs be exchanged without an IDX?	Yes. An FE can exchange EIDDs directly with other FEs. This might be implementation specific. In addition STA-010 specifies how to include an EIDD in a transferred call.
11.	Does the IDX act as a hub (similar to a location server) as opposed to a logger (after call time)?	The IDX is a live FE that acts as an aggregator and only keeps a current picture of an incident. It is not a store of historical information (e.g., if the address has changed three times then only the last change will be in the IDX).

Table 2: Q&A about what the Incident Data Exchange (IDX) is and is not.		
12.	EIDDs may have sensitive information, how is that information protected?	Security for EIDD exchanges is no different than any other exchange in i3. Credentials will be used for all EIDD exchanges (e.g., incident updates or requests for service setup). Requestor will identify and authenticate itself and the server will authenticate back to the requestor. Authorization and authentication is handled at the beginning of the exchange and credentials are used to filter based on policy. The Data Rights Management policy of the sender of the EIDD is the policy that is determinant as to what information is allowed to be exchanged.
13.	How does an FE that receives an EIDD send information it receives in an EIDD that it sends?	In general, FEs may not send information they receive from another entity. However, if an FE receives a reference to an EIDD (or a component of an FE) it may pass the reference on. Authentication of the requester is accomplished by the element providing the dereferenced value. If you dereference an EIDD or component to obtain a value, one should never forward the value, but only the reference URI. Dereferencing is always done at the host designated by the URI.
14.	Is dereferencing always done at the IDX?	The URI leads to some entity that will do the dereferencing, that may or may not be the IDX.
15.	What credentials are used by an FE (including an IDX)?	Any entity sending or receiving an EIDD must have credentials (i.e. public/private key pair issued within the Public Key Infrastructure (PKI) defined in STA-010)
16.	Does the IDX maintain a listing of EIDD related transactions?	No. The Logging Service performs this function.

	Table 2: Q&A about what the Incident Data Exchange (IDX) is and is not.	
17.	IDX vs. Logging Service: which element knows about every EIDD generated or distributed in/out of its domain?	The logging Service. The IDX keeps just a current picture of the incident to pass on to a subscriber.
18.	Is the incident record stored in IDX	An IDX may store current data for active incidents but does not store history.
19.	What about an Incident that spans more than one Agency?	When an Incident involves two or more Agencies, each Agency maintains their current view of the Incident which can be obtained from their IDX. Each agency has an IDX and a Logging Service. There is a way to discover all the Agencies involved in an incident and where the Logging Service and IDX for each of those agencies can be reached. There may be an Inter-Agency IDX, which is part of an NGCS, which coalesces information about a multi-Agency Incident from each of the constituent Agency involved and produces a single EIDD representing the aggregated current state of the Incident of all Agencies.
20.	How do you present full incident history to the call taker?	You get current incident state from the individual Functional Elements and/or the IDX (which aggregates incident data from multiple FEs). You get history from the Logging Service.

Table 2: Q&A about what the Incident Data Exchange (IDX) is and is not.		
21.	If an EIDD is only a snapshot in time, where are the EIDD transactions logged?"	In the Logging Service.
22.	If A transfers to B, would B then request the dereference function back through the IDX at A? If so, when B transfers to C, does C request the dereference function back through B or A?	An IDX may or may not be used. If an IDX is used, B gets an EIDD as part of the transfer. It could be by value or reference. If sent by reference, the URL you get tells you who can dereference it. It could be the IDX (that is implementation specific). For example, when A sends an EIDD 'by reference' to B, B goes back to A to dereference it. When B transfers the incident to C, if B send the EIDD by reference, then C goes back to B to dereference it. C will know that A is involved, and if C wants to find current state and to get updates, it will request those from A. When B transfers the incident to C, if B send the EIDD 'by value', then C doesn't need to dereference, but may still opt to request current state and updates from A.

Table 3: References		
REF 1.	From the APCO NENA spec, https://c.ymcdn.com/sites/www.nena.org/resource/resmgr/standards/APCO_NENA_2.105.1-2017_EIDD_.pdf	[from the section titled "Usage": The EIDD provides a standard for exchanging emergency incident related information. The EIDD represents the state of an emergency incident as known by a functional element or a single agency. An EIDD should be generated and exchanged among interested systems and stakeholders anytime that a significant change occurs in the incident's state. For example, among other possible triggers, an EIDD is generated and distributed anytime a 9-1-1 call is answered, a call taker enters notes about an incident, an emergency incident's location is established or changed, an incident is classified or reclassified (structure fire, vehicle accident with injuries, assault, etc.), emergency responders are dispatched, emergency responders arrive on scene, and when an emergency incident is closed with a final disposition. The EIDD provides information about the current state of an incident. It does not provide historical information about the incident. The Logging Service (see NENA-STA-010) is used to obtain historical information about an incident. An EIDD is usually associated with an active emergency incident. To support mutual and automatic aid, an EIDD can be used to report changes in an emergency responder's state without that EIDD being associated with an incident. EIDDs may contain sensitive and confidential information and should never be exchanged with another entity without first authenticating that entity and establishing its privileges (see NENA-STA-010, section 6.5: Authorization and Data Rights Management) to view the information contained in the EIDD. EIDDs may be filtered to remove sensitive and confidential information based on the authenticated privileges of the entity receiving the EIDD.
REF 2.	NENA-STA-010	NENA Detailed Functional and Interface Standards for the NENA i3 Solution