NUMBER: Six

SUBJECT: Confidentiality, disclosure and retention of 9-1-1 call[1] and other emergency information

OBJECTIVE: Ensuring that information delivered over Next Generation 9-1-1 systems can be appropriately delivered to Public Safety Answering Points (PSAPs) and shared with emergency response organizations while conforming to applicable confidentiality, disclosure and information retention statutes and rules

TARGET AUDIENCE: Congress and State legislatures; 9-1-1 Governing Authorities and other local rulemaking bodies; PSAPs and other emergency response agencies; National E9-1-1 Implementation and Coordination Office (ICO); Department of Health and Human Services (HHS); Department of Justice (DOJ); Department of Homeland Security (DHS); 9-1-1 service providers and vendors

JURISDICTION: Federal, State, Local

BACKGROUND AND DISCUSSION: Today's E9-1-1 systems are dedicated, closed, single purpose systems. The amount of information currently delivered with a landline, voice-over IP (VoIP) or wireless 9-1-1 call is limited compared with the information that will be available through NG9-1-1 systems. Since information associated with a 9-1-1 call in today's E9-1-1 system is generally stored in a single restricted location, preserving the confidentiality of the information and retaining appropriate records as required by local or state law is a relatively straight forward process.

Next Generation (NG) 9-1-1 systems will not be dedicated, closed, single purpose systems. They will be shared systems comprised of multiple entities. 9-1-1 will be only one part of a much larger system shared with general government, private sector entities and other public safety services/agencies. The amount and types of information (voice, text or video) that may be received by PSAPs and shared with emergency response agencies will greatly surpass current E9-1-1 systems. In addition to the increased amount of data, the nature of the content of data will be dramatically different in some instances. For example, NG9-1-1 will make it possible to transmit video, still images, medical information and a host of other data with a 9-1-1 call. Additionally, the architecture of NG9-1-1 systems will significantly increase the amount of data that is contained in shared databases with data residing in the network rather than in single-purpose databases housed locally. Finally, next generation systems can allow increased security of

[1] In this Transition Policy Brief, the term 9-1-1 emergency "call" refers to any real-time communication – voice, text or video and related data. The term also includes non-human-initiated automatic event alerts, such as alarms, telematics, or sensor data, which may also include real-time voice, text or video communications to a PSAP or other emergency response agency.

information through role-based access control and data rights management that limits access to information only to authorized entities. Existing local, state, and federal confidentiality, retention and disclosure laws were not designed to address these types of information and systems.

NG9-1-1 will make it possible to transfer the voice and data records associated with a 9-1-1 call, and ensuing actions in response, from the PSAP to other agencies, in real-time during an emergency, and to archive them (or portions of them) in a decentralized location (or locations) off site.

NG9-1-1 will make it possible for aggregate or anonymized information to be shared outside the bounds of the parties involved in the local response to a specific emergency. Governmental agencies such as the Centers for Disease Control, state/local health departments, state or federal departments of homeland security, emergency management agencies may have a legitimate need to be aware of a situation, and to have adequate information to assess the situation, anticipate what is likely to happen next, and decide what action(s) to take.

In this environment, states and the federal government need to be careful not to unnecessarily restrict access to critical emergency information. Privacy advocates and emergency responders can almost always agree on exceptions for life-saving situations, as they have done in the federal health records law, the Health Insurance Portability and Accountability Act (HIPPA), and with E9-1-1 location information in Section 222 of the Communications Act and comparable state laws. Similar exceptions to privacy laws for emergency purposes should be extended to all types of data. The last thing we want to do is limit the availability of information for which the NG9-1-1 system is specifically being designed to receive and share among authorized entities. Real time crash data from telematics/event data recorder systems in cars sent to 9-1-1 centers and emergency medical entities is a growing example.

Similarly, there need to be exceptions for legitimate research regarding improving end-to-end emergency response, assuming appropriate protections ensuring anonymous and aggregate use of data. For example, NG9-1-1 will make possible the collection and analysis of data from the beginning of an incident to the discharge of a patient from the hospital. Such data will enable research that will be invaluable in improving emergency response. Properly anonymized, it needs to be encouraged. In short, as NG9-1-1 systems are implemented that enable a much more data rich 9-1-1 and emergency response environment, laws should be crafted in a manner that enable the most effective real-time emergency response, as well as providing for appropriate anonymous data sharing, data mining and research.

ACTION PROPOSED TO RESOLVE ISSUE: 9-1-1 and emergency response authorities are encouraged to work with State Attorneys General, elected leaders and other stakeholders to:

- Ensure that a uniform and suitably broad definition of "9-1-1 call" is established in statutes and rules taking into account all types of information that may make up a 9-1-1 request for assistance.
- Analyze the applicability of current state confidentiality, disclosure and retention laws/rules to all types of 9-1-1 calls and call content and, as necessary, modify such laws/rules to treat all types of 9-1-1 calls and call content in a consistent manner.
- Ensure statutes and rules make clear the responsibility of all parties in situations in which 9-1-1 call information will be stored in non-local shared databases and networks.
- Ensure rules enable the simultaneous receipt of 9-1-1 call information from originators of such data by multiple emergency response agencies, as well as access to relevant information about individuals involved in emergency incidents, and the simultaneous sharing of such information among multiple authorized emergency response entities at all levels of government during and after incidents as appropriate. Sharing information with some parties in the chain of response, such as emergency operations centers (EOCs) or the Centers for Disease Control (CDC) may require anonymization of specific information in certain cases.
- Ensure that non-local agencies or local PSAP telecommunicators answering 9-1-1 calls outside of a physical PSAP (e.g. a virtual PSAP) may legally access 9-1-1 call data when necessary, while requiring adherence to appropriate confidentiality, disclosure and retention statutes and rules. This may require anonymization in certain cases.
- Require state and local 9-1-1 governing authorities to develop standard operating procedures (SOP's) establishing rules governing who has access to 9-1-1 call information, under what circumstances, and how they may be incorporated in data rights management, identity management and access control applications.
- Provide education and awareness of confidentiality issues in an NG9-1-1 environment for users of the system. The US Department of Commerce's National Institute of Standards and Technology (NIST) Special Publication 800-122 provides additional information that may be beneficial.