iCERT
Industry Council for Emergency Response Technologies

2017 Policy Platform

Overview

This document outlines the policy priorities for the Industry Council for Emergency Response Technologies (iCERT) for 2017, which represent the Association's focus for legislation, technology development, and regulatory matters throughout the year. For each of the below-noted issues, this platform outline includes a definition, iCERT objective or objectives, and the intended outcome or outcomes.

Inquiries regarding the iCERT policy platform for 2017 can be directed to George Rice, Executive Director, Industry Council for Emergency Response Technologies (iCERT) at george.rice@theindustrycouncil.org or 240-398-3065.

Issues

911 Governance & Accountability
Cybersecurity
NG911 Acceleration & Adoption
NG911/FirstNet Convergence & Data Interoperability
Targeted States Campaign – Resourcing of 911
Technology Transition and Obsolescence
Multi-Line Telephone Systems (MLTS): Access To 911

911 Governance & Accountability

Definition

The nation’s 911 services are rapidly changing. As Public Safety Answering Points (PSAPs) transition to new and more advanced next generation technologies, the underlying governance models, business models, and commercial relationships that form the basis of the 911 ecosystem are also transitioning. These changing roles and responsibilities require a careful review to ensure that best practices and regulations designed for legacy 911 systems are updated so that NG911 systems are highly reliable and resilient. Collaboration between and amongst vendors, public safety trade and practitioner associations, standards development organizations, public safety authorities and agencies, and federal, state and local governments is important in ensuring this goal is achieved.

Objective

Establish best practices and standards that recognize the evolving nature of the 911 ecosystem and ensure the reliability and resiliency of 911 systems and services.

Intended Outcomes

1. Increased awareness of the evolving 911 ecosystem among public safety and government stakeholders;
2. Development of best practices that improve 911 reliability and resiliency and improve coordination and communications between 911 service providers and public safety officials; and
3. Alignment of industry, public safety, and government stakeholders on the preference for collaboration and best practices over regulation.

Cybersecurity

Definition

The transition from voice-centric legacy public safety infrastructure to IP-centric NG911 underscores the need for a comprehensive cybersecurity framework that protects the security of these new, and in-transition, systems. The existing public safety infrastructure represents numerous systems that have been layered onto a staff constantly facing funding challenges and exposed to new cyber threats over a period of decades. While many agencies have not been afforded sufficient cybersecurity training, NG911 represents an opportunity to establish appropriate cybersecurity practices and to empower and properly size the technology staff.

Objective

Provide industry-based recommendations on cybersecurity guidelines, press for appropriate standards and technology architectures that highlight the broad public safety ecosystem encompassing NG911 and how it interacts with other public safety systems, identify methods for sharing active threat and mitigation information, and to promote effective and efficient funding for these initiatives from all levels of government.

Intended Outcomes

1. Increased awareness of the need for improved cybersecurity practices within public safety networks;
2. Development of best practices and standards that build upon existing studies from NIST, DHS, the FCC, APCO, NENA and others within the framework of existing standard-setting organizations;
3. Identification of needed funding and funding mechanisms that will support enhanced levels of cybersecurity practices from federal, state/local and industry sources;
4. Definition of appropriate policy and regulatory frameworks at federal, state and local levels that will promote a focus on cybersecurity needs and establish a responsibility for stakeholders to harden our public safety infrastructure;
5. Establishment of a framework in which to share sensitive cybersecurity threat information during active attacks and mitigation strategies that could help reduce the impact of a cybersecurity incident; and
6. Increased collaboration among industry partners and public safety stakeholders to improve the cybersecurity capabilities of our public safety agencies.

NG911 Acceleration & Adoption

Definition

The nation's 911 emergency communications system requires a transition from outdated and obsolete analog technologies to an IP-based infrastructure (NG911). NG911 will provide PSAPs with resiliency, redundancy, and call routing/transfer options that will improve the public's access to 911 in the time of an emergency. NG911 provides equal access to 911 for people with disabilities, domestic abuse victims, and other at-risk population groups in a manner that was inconceivable in an environment dominated by legacy technology. Importantly, with the increased availability of the "Internet of Things" (IoT), Smart Communities, and a dedicated broadband network for first responders, NG911 will also provide a path for vitally important public-initiated information to be used at the time of an emergency. However, the deployment of NG911 has been hindered by perceived challenges in governance, funding, technology and operations, as well as the lack of a targeted educational campaign highlighting the benefits of a nationwide deployment of NG911 and the consequences of a delayed transition.

Objectives

1. Provide a unified approach from our industry partners and public safety organizations to lead the transition from the legacy 911 environment to a nationwide deployment of NG911; and
2. Support the allocation of increased funding for NG911 and the education of stakeholders on the benefits of an accelerated deployment to NG911

Intended Outcome

Nationwide deployment of NG911 by 2020

NG911/FirstNet Convergence & Data Interoperability

Definition

Public safety authorities, and the commercial enterprises that provide them with technology products and services, are looking to fully understand the nature and extent of expected synergies and convergences between NG911 and public safety broadband systems. The full continuum of services, beginning with – by example – a 911 caller sending a smartphone image through a state's Emergency Services IP Network (ESINet) and out to first responders via FirstNet, is in need of comprehensive and deliberate planning in order to ensure that all aspects of this emergency communications continuum are fully coordinated, funded, standards-compliant, and secure.

Objective

Provide policymakers, public safety agencies, and other affected stakeholders with industry guidance on how NG911 networks must be integrated with the nationwide public safety broadband network being developed by FirstNet. In addition, identify what standards and best practices must be developed to ensure interoperability of data that traverses those networks, and the key components of funding responsibility, so that new NG911 systems can be implemented in an effective and efficient manner.

Intended Outcomes

1. A non-technical illustration of the full process associated with the emergency calling and response continuum, and the points at which a particular funding source(s) provide support for these services (to be used by elected officials and other non-technical government administrators and authorities); and
2. Specifications for standards development organizations to use to create a data interoperability standard across public safety data management and dissemination systems.

Targeted States Campaign – Resourcing of 911

Definition

Funding for 911 systems and programs is often inadequate to support the services that must be delivered, sometimes due to diversion of collected 911 fees to unrelated functions. Absent appropriate levels of stable and foreseeable funding for emergency calling the nation's 911 system breaks down. Public safety officials become unable to procure the equipment and services they need in order to provide safety at the level the public deserves and expects. When properly resourced, however, public safety agencies can meet their goals, and provide to the public the crucial life-saving services our citizens, residents and visitors require.

Objective

As part of a state-by-state program, secure and protect 911 funding consistent with iCERT's funding principles, and work in conjunction with state and local officials to provide much needed resources to initiate, maintain, and/or bring to fruition state-level efforts to ensure that emergency calling is properly resourced in America.

Intended Outcome

1. Shifts in norms - reduced state reliance on 911 funding for unrelated matters;
2. Strengthened organizations - general increase in 911 agency budgets due to regular transfer of dedicated funding;
3. Improved policies - states amending regulations and/or administrative practices to ensure flow of funding; and
4. Specific impacts - key examples of appropriately repositioned funding in states.

Technology Transition and Obsolescence

Definition

Consumers and businesses are rapidly adopting new communications technologies, including IP-based technologies. iCERT believes that the widespread adoption of these advanced technologies and the transition to an all-IP network will yield numerous benefits for public safety. Yet, public safety agencies are faced with budget constraints that are very different than commercial enterprises and are often unable to adopt new technologies as rapidly as the private sector. Consequently they are faced with the need to maintain long-serving, yet aging, equipment that entails significant technology obsolescence risk.

Objective

Promote the timely adoption of new technologies among public safety agencies by demonstrating the benefits of technological innovation and the risks of keeping technology past the point of obsolescence and establishing funding mechanisms that enable technological advancements to be implemented.

Intended Outcome

1. Increased awareness among public safety agencies and other stakeholders of the risks associated with technological obsolescence and the benefits of technological innovation;
2. Establishment of funding mechanisms that enable technological advancements to be implemented when they are needed and available; and
3. Broad adoption of new technologies by public safety agencies, consistent with broader marketplace trends.

Multi-Line Telephone Systems (MLTS): Access To 911

Definition

Effective access to 911 service in businesses, dormitories, multi-tenant dwellings, hotels, and other temporary lodgings is essential to the safety of life and property throughout America. However, many MLTS systems do not offer ease of access to 911.

Consumers traveling for business or leisure often frequent hotels and other temporary lodgings served by MLTS, and are generally unaware of system limitations that can prevent direct access to 911 or hinder the ability of 911 and first responders to locate callers utilizing a hotel MLTS system.

Many employers also operate MLTS where service footprints may extend across cities, counties, or state lines and service multiple locations or campuses, and employees often do not realize that 911 calls from these facilities could be routed to the wrong Public Safety Answering Point (PSAP), or intercepted before ever reaching authorized local response agencies.

Objective

Support state and federal public policy that requires direct dial access to 911 for calls placed within a Multi-Line Telephone System, including providing public safety with an accurate call-back telephone number and location/dispatchable address.

Intended Outcomes

1. Increased awareness that MLTS systems remain the only telecommunications device accessing the public switched telephone network that is not required to:
   - Provide direct access to 911;
   - Route a 911 call to the closest and appropriate PSAP; or
   - Provide a PSAP with a call-back telephone number, or location/dispatchable address.
2. Establishment of requirements for the manufacture, importation, sale, installation, configuration, and maintenance of Multi-Line Telephone Systems
3. Establishment of certain liability protections for manufacturers, service providers, and system managers as appropriate;

# # #

Adopted and Approved by the iCERT Board of Directors on March 1, 2017