iCERT
Industry Council for Emergency Response Technologies

2019 Policy Platform

Overview

U.S. consumers and businesses are rapidly adopting new communications products and services that are increasingly mobile, data-centric, and bandwidth-intensive. These trends are driving new innovations in areas like 5G Mobility, Internet-of-Things (IoT), Virtual Reality/Augmented Reality, and Cloud Computing. 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 as well. Agencies are already adopting LTE mobile technology and looking to integrate these new solutions with their land mobile radio (LMR) systems. In the future, the implementation of Next Generation 911 and the adoption of IoT and cloud-based solutions for public safety will enable 911 personnel and first responders to fully leverage a wide array of data available to improve situational awareness and emergency response.

Unfortunately, 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. As a result, they are often faced with the need to maintain long-serving, yet aging, equipment that entails significant technology obsolescence risk.

This document outlines iCERT's 2019 policy priorities; policies designed to address critical funding challenges and promote an environment that enables public safety to fully leverage technological innovation. Inquiries regarding this document can be directed to Kim Scovill, iCERT Executive Director, at executivedirector@theindustrycouncil.org or (202) 503-9998.

Adequate and Sustainable 911 Funding

Description

Funding for 911 systems and programs is often inadequate to support the services that must be delivered. In some cases, the lack of sufficient funding can be attributed to outdated funding policies that have not kept pace with technological and marketplace changes. In other cases, funding is unavailable due to diversion of collected 911 fees to unrelated functions. These funding challenges place our nation's 911 systems, and the public, at risk by making it difficult for public safety officials to procure the equipment and services that are necessary to support emergency calling services. State and local 911 policies must ensure a stable and sufficient level of funding in order to support the crucial life-saving services our citizens, residents and visitors require.

Objective

Work in conjunction with state and local officials to secure and protect 911 funding consistent with iCERT's principles,[1] and work to ensure that money collected for 911 is not used for other purposes.

Desired Actions

1. Support efforts to discourage and/or prohibit the diversion of 911 funds for unrelated purposes.
2. Support efforts to increase direct dedicated funding for 911 services;
3. Promote state and local policy frameworks that ensures 911 funding keeps pace with technological and marketplace changes; and
4. Work with policymakers and stakeholders to advance new 911 funding statutes and regulations, consistent with iCERT's funding principles.

[1] *iCERT 911 Funding Principles*, released 2014.

Nationwide NG911 Deployment

Description

The nation's 911 emergency communications systems require a transition from outdated and obsolete technologies to an IP-based Next Generation 911 (NG911) infrastructure. NG911 will enable the public to access 911 services through a variety of non-voice modes of communications, provide first responders with increased access to data that will improve situational awareness, and provide Emergency Communications Centers (ECCs) with greater resiliency and call routing/transfer capability. The wide deployment of NG911, however, has been hindered by limited funding and a lack of national leadership that places a high priority on updating the nation's 911 systems.

Objective

Establish a national policy framework that makes accelerated NG911 implementation a high priority and provides significant Federal funding to support nationwide deployment.

Desired Actions

1. Establish a unified public safety and industry coalition committed to the accelerated implementation of NG911 systems and services; and
2. Enact Federal legislation that establishes a national framework for NG911 and provides significant funding to support nationwide deployment.

Conformance to NG911 Standards

Description

The deployment of NG911 nationwide is a principal goal of iCERT's 2019 Policy Platform. Interoperability between NG911 systems deployed by counties, regions, or states is critical, and interoperability challenges may be one impediment to achieving this nationwide deployment goal. A second challenge is the interoperability between the Originating Service Providers (OSPs) and NG911 systems. Finally, some 911 authorities lack the technical capability to evaluate NG911 services offered by vendors. All three of these challenges can be somewhat mitigated by the implementation of a testing protocol to validate conformance to applicable standards.

Conformance to standards and assurance of interoperability is also viewed as a prerequisite to obtaining additional Federal funding for the migration to NG911; another key policy objective of iCERT for 2019. iCERT supports legislation that makes interoperability a condition of Federal NG911 grants, and the testing protocol envisioned by iCERT would help address this issue.

The iCERT NG911 Conformance Working Group will focus on deliverables that help facilitate the implementation of a testing protocol consistent with iCERT's principles.

Objective

Promote conformance to NG911 standards through the development and implementation of a testing protocol.

Desired Actions

1. Work with recognized standards development organizations and various stakeholders, as appropriate, to promote interoperability through ongoing, multi-vendor conformance to standards, and associated testing, that ultimately provides end customer confidence in heterogeneous deployments.

2. Create educational content and guidelines that aid in reaching and maintaining conformance.

Data Sharing between NG911 and Public Safety Broadband Systems

Description

The rapid adoption of wireless broadband technologies by public safety enables first responders to communicate more effectively and to make greater use of an increasing array of data to improve situational awareness and emergency response. The accelerated deployment of NG911 will enable the nation's 911 emergency communications centers to achieve similar benefits by leveraging data provided by 911 callers. In order for these advanced capabilities to provide the most benefit, however, data must be shared between the NG911 systems used by Emergency Communications Centers (ECCs) and the public safety broadband networks used by First Responders. Collaborative efforts on the part of public safety authorities and industry representatives are necessary to ensure that all aspects of the emergency communications continuum are fully coordinated, funded, standards-compliant, interoperable, and secure.

Objective

Promote the effective sharing of data between NG911 networks and public safety broadband networks and the interoperability of data flows between and across those networks.

Desired Actions

1. Provide policymakers, public safety agencies, and other affected stakeholders with industry guidance on how NG911 networks can be used to share data with first responders and how specific funding sources are used to support these services; and
2. Promote the development of standards and best practices that facilitate the interoperability of NG911 systems and the sharing of data transmitted across NG911 and public safety broadband networks.

Cybersecurity Protections

Description

The transition of the nation's public safety communications systems from a voice-centric infrastructure to a data-centric, IP-based infrastructure underscores the need for a comprehensive cybersecurity framework that protects the security of these new, and in-transition, systems. This evolving infrastructure presents public safety officials with new potential threats for cyber-based attacks, as well as new ways to protect against those attacks. As IP-based public safety communications systems are implemented nationwide, public safety officials and industry representatives need to work together to establish appropriate cybersecurity practices and ensure that emergency personnel are properly trained to protect the security of the nation's emergency response systems.

Objective

Promote a public policy framework and communications ecosystem that anticipates the potential for cyber-based threats and promotes effective protection of public safety networks, services, and applications through best practices, training, increased information sharing, and broad collaboration with affected stakeholders.

Desired Actions

1. Increase awareness of the need for improved cybersecurity practices and hygiene within public safety networks;
2. Collaborate with public safety and other stakeholders to develop best practices and standards that help to protect public safety networks, services, and applications. Build upon existing studies from NIST, DHS, the FCC, APCO, NENA and others within the framework of existing standard-setting organizations;
3. Promote cybersecurity training for public safety personnel, encourage situational awareness and generate cyber incidence response and preparedness;
4. Identify cybersecurity funding requirements and secure increased funding from federal, state and/or local sources to support enhanced levels of cybersecurity protections;
5. Advocate a policy framework that will promote effective cybersecurity protections without impeding technological innovation; and
6. Support frameworks that facilitate the sharing of sensitive cybersecurity threat information during active attacks and mitigation strategies that could help reduce the impact of a cybersecurity incident.

Investing in Smart and Safe Communities

Description

A "smart community" is a locality that has developed a technological infrastructure that enables it to collect, aggregate, and analyze real-time and stored data, and uses that data and associated technologies to increase efficiencies, improve sustainability, spur economic growth, and enhance the lives of its residents. The concept of a "safe community," in relation to a smart community, has been developed to help government administrators and first responders leverage advanced communications technologies and increased access to information in order to promote public safety. This includes promoting greater connectivity across all public safety systems, leveraging data through predictive analytics, and developing real-time response procedures and advanced emergency response systems to better serve communities, their citizens, residents, and visitors.

Objective

Educate policymakers and key stakeholders on the importance of investing in technologies and related infrastructure that support "smart and safe communities," highlight the importance of such investments to public safety, and demonstrate how NG911, 5G Mobility, IoT for Public Safety, Cloud Computing, and similar initiatives are critical to achieving both smart and safe communities.

Desired Actions

1. Promote public policies that increase advanced communications infrastructure investments and promote efforts to enhance collection and use of data to predict and respond to incidents.
2. Increase awareness and education regarding the useful synergies among the various types of information gathered and utilized by communities – both public and private – with attention toward heightened analysis of this data for public safety use with due attention to privacy matters.

# # #

Revised and Approved by the iCERT Board of Directors on June 17, 2019