The Computerworld Honors Program

Honoring those who use Information Technology to benefit society

Final Copy of Case Study

Status:
Laureate

Year:
2013

Organization Name:
Jersey City Office of Emergency Management & Homeland Security

Organization URL:
http://www.cityofjerseycity.com/emergency.aspx?id=7970

Project Name:
Jersey City IRAPP

Please select the category in which you are submitting your entry:
Safety & Security

Please provide an overview of the nominated project. Describe the problem it was intended to solve, the technology or approach used, how it was innovative and any technical or other challenges that had to be overcome for successful implementation and adoption. (In 300 words or less.)

A National Interoperable Communications Platform. Despite a decade of significant investments and concerted efforts, a pervasive, national communications interoperability solution for emergency response has remained a bridge too far with, at best, small pockets of interoperable communications ability existing among a few select agencies. Emergency events such as the World Trade Center attacks, the Columbine School shootings, Hurricane Katrina, the Deepwater Horizon oil spill, the Aurora, CO movie theater shootings and host of other natural, accidental and man-made incidents exposed and will continue to expose the persistent and prevailing problem of a lack of effective coordinated communications between first responders and other emergency support and critical infrastructure organizations that are critical to responding to, mitigating

and recovering from disasters. Perhaps we have been trying to solve the wrong problem, or at least we have been trying to solve it the wrong way. A broad-based national interoperable communications and multimedia collaboration platform can be achieved quickly and affordably through an everything-over-IP (EOIP) sovereign-controlled, peer-based virtual network. This approach leverages existing communications and media infrastructure as well as next generation broadband efforts, such as FirstNet, to create an adaptive, resilient and scalable collaboration framework that achieves ubiquitous capabilities among first responders as well as critical infrastructure entities. Challenges: Tremendous amounts of communications media infrastructure (radio, video, mobile communications, sensory information, telephony, data files and chat) exist in disconnected silos in both vertical (large hierarchical organizations) and across horizontal (cross-agency, critical infrastructure partners) environments. Usually, all of these varied communications and media assets are controlled by the owners, whether local, state or federal sovereign government entities, or private owners. Each of these owners is unlikely to relinquish control over critical communication resources. Security of the sharing environment, regulatory restrictions and privacy issues are also challenges.

When was this project implemented or last updated? (Please specify month and year.) Has it incorporated new technologies and/or other innovations since its initial deployment? (In 300 words or less.)

Mutualink began installing platform endpoints in 2006; as of Dec. 31, 2012 the Interoperable Response and Preparedness Platform (IRAPP) comprises over 1,000 endpoints. The technology has evolved with software improvements and upgrades over the years. 2012 saw the use of the platform in conjunction with LTE (long-term evolution) to provide an even more inclusive network to benefit first responders.

Is implementation of the project complete? If no, please describe the project's phases and which phase the project is now in. (In 300 words or less.)

The nature of the IRAPP is such that it will never be "complete." New users, participants and endpoints are being added constantly. The IRAPP is fully functional and has been in use for five years. Platform enhancements flow in as technology evolves, with continuous improvements.

Please provide at least one example of how the technology project has benefited a specific individual or organization. Feel free to include personal quotes from individuals who have directly benefited from the work. (In 300 words or less.)

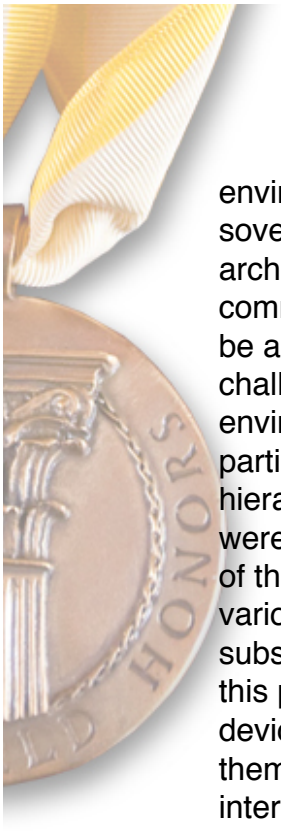
The state of New Jersey felt the full force of Hurricane Sandy on October 29, 2012. In Jersey City, only 14.3 square miles is land, out of a total of 22 square miles. The City flooded with a vengeance. By the time Hurricane Sandy hit Jersey City, 165 state and local government agencies and private enterprises comprised the IRAPP, among them, Atlantic City casinos, state and town Office of Emergency Management (OEMs), stadiums, police departments (state and local), fire departments, hospitals and malls. By mid-morning on Oct. 29, agencies on the IRAPP were calling in to their Mutualink Field Trainer for a "comms check" to ensure full and proper functioning of their equipment and the IRAPP. Agencies who did not initiate a call were contacted for the same. For the Jersey City Office of Emergency Management, Sandy provided the third major incident, following Hurricane Irene in 2011 and the "Miracle on the Hudson" emergency landing of US Airways' Flight 1549 in 2009, for which the IRAPP provided interoperable communications capabilities. During the emergency plane landing, Jersey City first responders were able to send video from the crash site to local hospitals, giving them a decent idea of how many incapacitated people they could expect. During Sandy, hospitals utilized the IRAPP to coordinate with public safety agencies during evacuations, as water levels rose and proved a threat to their facilities. Video feeds enabled Jersey City OEM to follow the surge of water as it progressed from Atlantic City northward. Hospitals kept informed in real time regarding the operations at other hospitals and shared information with the Jersey City OEM.

Would this project be considered an innovation, a best practice or other notable advancement that could be adopted by or tailored for other organizations and uses? If yes, please describe that here. (In 300 words or less.)

This project represents a best practice based on an innovative use of technology that is deployable nationwide, as well as among our troops and their partners and allies abroad. The IRAPP utilizes a plug-and-play technology, making it accessible and affordable for both the government and private sectors.

If there are any other details that the judges should know about this project, please note them here. (In 300 words or less.)

Two of the primary and substantial challenges in making entities willing to participate in multi-agency interoperable environments are: respecting the sovereignty of their communication resources and ensuring a secure



environment over which those resources may be shared. One way that the sovereignty of control of resources can be assured is through the fundamental architecture of the system that connects them. A classic approach to communication network design is the "hub and spoke." While this can certainly be a fine technical solution, it does not address some of the key human challenges to attaining a multi-agency interoperable communications environment. Principally, it does not respect the sovereignty of the individual participants' own communications assets because one of the entities is hierarchically superior (hub) to the others (spokes). If, in such a system, one were to remove the controlling central hub and place the control and intelligence of the system out at the (their) edge, proximate to each of the owners of the various communication resources, a network of peers would emerge, substantially mitigating concerns regarding control sovereignty. Furthermore, in this peer-to-peer environment, through technology, each communication endpoint device is knowledgeable of all other endpoints and knows how to directly reach them and establish a communications path between them without the aid of an intermediary host server. As for the issue of security, it can be addressed in three categories: platform or operating system (OS); validation of participants; and transport mechanism. An environment having a secure OS, utilizing a dynamic Public Key Infrastructure (PKI)10 to mutually and securely validate participants, and wrapping the transport in encrypted tunnels would address security concerns of the participants. Taken together, these technical attributes serve as the foundation upon which a large-scale capability can be built.