New Capabilities for Public Safety: Enhancing Emergency Response and Day-to-Day Operations

Abstract
Communication and collaboration form the cornerstone of public safety agencies’ ability to protect lives, property, and infrastructure. The agency’s communications technology plays an increasingly important role in the effectiveness of emergency response and day-to-day operations. Specifically, agencies need communications interoperability, the ability to traverse jurisdictional “silos” of information, protection against premature technology obsolescence, and effective use of human capital. Public safety agencies around the world are successfully addressing these requirements with the following initiatives:

• Communications interoperability: Emergency response and day-to-day operations improve when first responders and incident commanders can communicate directly using any radio system as well as with a traditional phone, IP phone, cell phone, or PC client.

• Effective incident management: Large-scale disasters and crimes as well as major events such as sporting tournaments require unified command and control. Incident commanders need the ability to communicate with personnel from multiple agencies on the scene, and to command as effectively from home or mobile command posts as they can from headquarters.

• Enhanced mobility: With secure, outdoor wireless access to departmental applications and databases, public safety personnel can receive voice, video, and data services at the point of need and share video with headquarters and first responders. In law enforcement, wireless networks act as a force multiplier by enabling officers to remain in the field rather than driving back and forth to and from the office.

• Disaster recovery and continuity of government: Public safety personnel need the ability to quickly reconstitute voice and data communications when the infrastructure is destroyed, damaged, or overwhelmed. In addition, the communications infrastructure must remain operational even if dispatchers and other personnel are prevented from working in the office, as in the case of flu pandemic.

• Optimized use of human capital: Public safety agencies compete with other public and private sector organizations for the best personnel. They gain a competitive advantage in recruitment and retention when they provide personnel with technology that helps them perform their jobs effectively and remain safe.

Public safety agencies around the world are meeting these goals today with Cisco® solutions for the core network, unified communications, and wireless access.
Communications Interoperability

**Goal:** Provide easy-to-use, cost-effective, comprehensive communications interoperability across departments and jurisdictions.

Lack of interoperable communications among different first-responder organizations leads to uncoordinated response and a fragmented chain of command. These, in turn, can hinder the ability to save lives, property, and infrastructure. Lack of interoperability also impedes day-to-day operations ranging from Amber alerts to hurricane response. These incidents typically require response from multiagency task forces, possibly including government agencies, private assistance groups, and enterprises, all of which typically use incompatible radio systems.

By sending radio traffic over the government’s existing IP network, the Cisco IP Interoperability and Collaboration System (IPICS) solves the interoperability challenge. Cisco IPICS provides cost-effective and comprehensive communications interoperability between push-to-talk (PTT) radio systems as well as devices such as mobile phones, IP phones, public switched telephone network (PSTN) phones, and PC clients. The ability to use any type of radio enables agencies to extend the life of current investments while gaining the flexibility to add new types of communications devices as technology and public safety requirements change. Based on proven IP standards, Cisco IPICS takes advantage of ubiquitous IP networks to extend the reach of traditional communications networks and to provide notification using email, pager notification, and Short Message Service (SMS). Comprehensive communications interoperability enables public sector agencies and enterprises to intelligently apply their resources to streamline operations and to improve incident response.

The Boulder County, Colorado Sheriff’s Office uses Cisco IPICS to set up virtual talk groups that preauthorized participants can join using a VHF radio system, any other radio system, cell phone, IP phone, traditional phone, or PC with Cisco PTT Management Center Client software. The county’s SWAT teams have used Cisco IPICS to facilitate negotiations with suspects. They patch the suspect’s phone or cell phone into an operational or tactical radio channel, and the negotiator joins in using either a radio or cell phone.

Effective Incident Management and Major Events Hosting

**Goal:** Achieve unified command and control during large-scale disasters and crimes as well as major events.

Today’s fragmented approach to incident management can contribute to a breakdown of command and control. Decision making is delayed when commanders need different devices to communicate with field personnel, access databases, and view sensor information. Workarounds such as maintaining a cache of radios for distribution to other agencies that convene on the incident scene are expensive and do not scale well. Agencies need more predictable methods to comply with the National Incident Management System as specified in the Homeland Security Presidential Directive 7 (HSPD-7).

Cisco wireless solutions and Cisco Unified Communications solutions facilitate unified command and control, improving situational awareness for field personnel and increasing the speed of the decision-making loop. With a converged Cisco network, incident commanders can gain a consolidated view of all application and sensor information they need to make informed decisions:

- Sensor data: From a PC or laptop in the field, commanders can connect over the Cisco outdoor wireless mesh network to monitor sensor readings as well as view sound- or motion-activated video. Types of sensor data useful for incident management can include weather, gunshots, chemical, biological, radiation, explosives, and other (Figure 1).
- Streaming video: Cisco video solutions enable decision makers to actually see what is happening at the incident scene rather than relying on verbal descriptions. In the United Kingdom, the Humberside Police Department transmits aerial video images of major incidents from its helicopters to a specialized control center. A Cisco IP/TV® system broadcasts the video footage over the departmental intranet to other police stations throughout the jurisdiction, where officers can view them from a Web browser to make more informed decisions.
Communicating with the “Tip of the Spear”

Effective crime prevention, protection of life and property, and crisis management depend on collaboration and timely delivery of actionable information to the “tip of the spear,” the personnel at the scene or in the field. These personnel are farthest removed from law enforcement and public safety information and yet must make decisions that affect public safety, such as:

- Should I arrest this individual?
- Am I dealing with terrorism?
- Should I call for backup?

By making it easier and faster to deliver information to personnel at the tip of the spear, Cisco outdoor wireless solutions and Cisco Unified Communications solutions increase the value and speed of information.

Enhancing Emergency Operations

Used during emergency situations, Cisco Unified Communications solutions can:

- Provide remote access to IP video surveillance and dispatch, improving situational awareness for first responders and thereby increasing safety for both the responders and the citizens they protect
- Enable effective crisis management by connecting response teams to command personnel through a voice, video, and Web conference where they can plan joint actions
- Broadcast vital voice and data alerts, such as Amber alerts, natural disasters, and elevated threat levels, to employees’ IP phones, cellular phones, PDAs, and other devices
- Establish an efficient contact center with flexible call-routing options to handle rising call volumes associated with major incidents, natural disasters, terrorism threats, and mass disturbances

Communications interoperability: Cisco IPICS provides comprehensive communications interoperability, facilitating interagency collaboration, improving situational awareness, and speeding up the decision-making loop. Incident response improves when public safety agencies can intelligently apply resources and rapidly respond to routine events as well as emergencies.

Figure 1 Unified Command and Control

Goal: Enable field personnel to access actionable information from the field as if they were in the office.

Today, departmental applications such as computer-aided dispatch and records management systems can only be used within the building walls. Field personnel who need to access these applications or submit reports must drive back to the precinct, reducing their presence on the streets.

Cisco wireless solutions and security technologies enable law enforcement, fire, and emergency medical services personnel to access applications and databases from the field rather than driving back to the office. In cities with Cisco outdoor wireless mesh networks, personnel can use a laptop or personal digital assistant (PDA) in any area to access databases, submit reports, or print citations. Cities that have not yet deployed an outdoor wireless mesh network can establish wireless hotspots in the parking lots of government buildings so that officers can access the network from their vehicles. Cisco encryption technologies protect information from eavesdropping, and Cisco Network Access Control technologies authenticate personnel and provide role-based access, protecting citizen and government privacy.

Disaster Recovery and Continuity of Operations

Goal: Provide first responders with easy-to-use tools to quickly reconstitute voice and data networks and ensure that the chain of command remains operational even if the infrastructure is destroyed.

Effective command and control during emergencies require communications between headquarters and the field, even when the communications infrastructure is destroyed, degraded, or overwhelmed. Causes can include natural or manmade disasters, power outages, weather-related incidents, terrorist strikes, or avian flu pandemic. Cisco solutions facilitate disaster recovery in the following ways:

- Public safety agencies need the ability to immediately reconstitute communications if
the network is unavailable or to establish communications if there is no infrastructure. With Cisco Rapidly Deployable Communications solutions, a first responder can simply flip a switch to connect to the IP network by satellite, if needed, or to existing wired or wireless networks. The solution creates an instant network that personnel in the vicinity can use to send and receive voice, video, and data, using wired or wireless devices. The iComm kit is designed for agency-level support, and the suitcase-sized Tactical Communications Kit, from Cisco and its partner CACI, is designed for small groups. Both can withstand harsh conditions.

• Increased span of control: Cisco IPICS provides comprehensive communications interoperability, with PSTN phones as well as radios.

• Resilient communications infrastructure: Public safety agencies that integrate their communications infrastructure with the government’s Cisco IP network improve their disaster recovery capabilities. If the physical offices become inaccessible for any reason, the agency can reestablish operations in any other location that has wired, wireless, or satellite network access.

• Mobile command vehicles: Using the Cisco Metropolitan Mobile Network solution, for which Cisco received the Frost & Sullivan Technology Leadership Award for wireless solutions for first responders, agencies can establish emergency communications in mobile command vehicles. The City of Everett, Washington Police Department uses the solution to transform its vehicles into mobile command posts, using in-vehicle Cisco 3200 Series Wireless and Mobile Routers that connect over the city’s Cisco outdoor wireless mesh network.

• Distributed contact centers: Cisco Unified Contact Center enables distributed contact center operations by routing calls to available agents in any location, including their homes. When an ice storm struck north Texas, the state’s 2-1-1 contact center continued to function even though personnel in four cities could not travel to the office to take calls. The agency simply configured the system to forward calls to the backup center, enabling uninterrupted service.

• Secure remote access: Public safety agencies create a resilient workforce by providing essential personnel with Cisco VPN solutions and Cisco Unified IP Phones at home. Using a PC and broadband connection, employees can securely access their department’s voice and data services. Calls to an employee’s office phone number ring on the home IP phone. The same solution enhances day-to-day operations, avoiding the unreliability of emergency processes that are used infrequently.

• Cisco TelePresence: For high-level decision making during emergencies, public safety agency executives can collaborate remotely as if they were face to face, using Cisco TelePresence. Meeting participants see life-size images of remote participants, with fluid motion and ultra-high definition that reveals subtle facial expressions as if the other person were seated across the table rather than thousands of miles away.

Optimized Use of Human Capital

Goal: Attract the best and brightest personnel and use them effectively.

Public safety agencies compete for talented employees with private sector as well as other public sector agencies. Candidates prefer to work for agencies in which they can focus more on public safety and spend less time in the office filing reports. Cisco technologies for communication and collaboration help public safety agencies make themselves more attractive to new and existing employees. With outdoor wireless mesh networks, for example, law enforcement personnel can access criminal databases and mug shots from the field, at the point of need, enabling them to spend more time in the field and less driving back and forth to and from the office. Fire fighters can access hazardous materials databases and floor plans from their vehicles while driving to a fire, increasing situational awareness as well as their own safety. Cisco IPICS enables first responders to communicate with personnel from other agencies, increasing situational awareness and safety.

Cisco Solutions for Public Safety

Cisco Core Foundation

A Cisco Service-Oriented Network Architecture forms the basis for services that increase
situational awareness for first responders and increase the speed of the decision-making loop. Multiple public safety agencies and government departments can share the costs of a network infrastructure. Cisco Self-Defending Network technologies protect the network from unauthorized access, infections, and theft of information, ensuring continuity of government. Other Cisco security technologies enable jurisdictions to share information when appropriate, such as when responding to interjurisdictional crimes, and keep it private otherwise. The network has the intelligence to enforce each agency’s policies for access control and data protection.

Benefits of Cisco core foundation technologies for public safety include:

- Network simplification and increased responsiveness: With a secure Cisco core foundation, public safety agencies can deliver voice, video, and data services to first responders and incident commanders over a converged network. Reducing the number of networks to maintain reduces capital and operational expense and enables public safety agencies to adapt more quickly to new needs in a changing world. The Cisco core foundation also provides the basis for Cisco Unified Communications and wireless services.

- Secure information sharing between departments and jurisdictions: By enabling commanders to securely access information from multiple information systems from their office, at home, or during travel, the Cisco secure access technologies facilitate distributed command and control.

- Ability to deliver rich content: Cisco networks provide the quality of service to support voice, video, and data on the same network. The fire department can transmit video to a monitor in the fire vehicle as it travels to a fire, for example, increasing situational awareness.

- Security: Cisco access technologies protect employee and citizen privacy and ensure compliance with legislative mandates.

Cisco Unified Communications

Cisco Unified Communications solutions address a broad spectrum of public safety communications requirements. IP telephony, voicemail, and collaboration solutions help improve communication and teamwork while reducing costs. Advanced call-processing and contact center solutions increase the capabilities and resiliency of the communications infrastructure. Cisco video telephony and Cisco TelePresence solutions integrate video into communications, reducing the need for travel and enabling high-level discussions when personnel are isolated during a flu pandemic or other events that restrict travel. Low-cost, IP-based video surveillance serves as another force multiplier, enabling 24-hour monitoring of high-crime areas from any location with a Web browser. Cisco mobile voice solutions enable public safety agencies to rapidly establish voice and data communications in any location, connecting to the agency network through an existing wired or wireless network or by satellite.

Benefits of Cisco Unified Communications for public safety include:

- Reduced costs: Cisco Unified Communications reduces total cost of ownership compared to private branch exchange (PBX) systems and Centrex.

- Greater responsiveness for increased public safety: Features such as four-digit call transferring and online directories improve productivity. Cisco presence technology indicates which experts in a particular agency are available right now and how to reach them. The employee can drag the name of available resources into a collaborative workspace in Cisco Unified MeetingPlace® to initiate a recorded voice, video, and Web conference (Figure 2).

- Rich media: The department can use its network for digital video as well as for voice and data. Training becomes more cost-effective when supervisors can train remote employees using Cisco Unified MeetingPlace, which combines voice, video, and Web collaboration. In Arlington County, Virginia, the fire department uses Cisco video solutions to broadcast a real-time training broadcast directly to each fire station, avoiding the time and expense of creating and delivering multiple copies of a videotape.

- Improved citizen services by providing a single phone number to contact any government agency: With Cisco Unified Contact Center, state and local governments can provide a single nonemergency number, either a seven-digit number or 3-1-1, that citizens can call for referral to any service they need.
Cisco Wireless Solutions

First responders increase their situational awareness and productivity with Cisco wireless solutions:

- Cisco indoor wireless solutions enable headquarters personnel to access departmental voice, video, or data services from any indoor area or adjacent outdoor area, improving productivity and service effectiveness.
- Hotspots and building-to-building connectivity extend wireless access to parking lots, walkways, and other areas adjacent to buildings. Law enforcement and other public safety personnel can access drivers’ license information, mug shots, and criminal databases from the parking lot of any government building rather than driving back to the precinct, increasing their presence on the streets.
- Outdoor wireless mesh solutions deliver broadband connections to metropolitan-area environments. Law enforcement, fire, and emergency medical services personnel whose vehicles are equipped with Cisco mobile access routers can access blueprints, hazardous materials information, warrant information, and more, enhancing public safety.

Conclusion

New challenges for public safety include surmounting interoperability issues, enabling information sharing across departmental and jurisdictional boundaries, avoiding technology obsolescence, and attracting the best and brightest personnel. Cisco solutions meet these challenges by providing comprehensive communications interoperability, increasing situational awareness, increasing the speed of the decision-making loop, and facilitating disaster recovery and continuity of government. The benefits apply to day-to-day operations as well as emergencies.

For more information about Cisco solutions for public safety, visit http://www.cisco.com/go/publicsafety