Providing access to information to those who need it most, when they need it most, is on virtually every agency’s agenda, no matter what their size or location. Driven by this desire to access and share data – real-time video, suspect photos, database information and more – the interest in mobile broadband is clearly shown in Motorola’s recently completed 2013 public safety communications survey. The study also reveals the attention that government agencies are giving to cybersecurity and the devices that deliver data to the field.

**INCREASED INTEREST IN HIGH-SPEED DATA ACCESS**

Why is high-speed data access so important? It enables first responders to make more informed decisions to better serve the public and protect lives. While the Public Safety Industry Study survey conducted by Motorola in 2012 documented the emerging emphasis on data communications in public safety, the new 2013 study is notable for showing how quickly the trend of providing mobile broadband access in the field is escalating. Responses revealed that in the last year, the number of agencies acknowledging the importance of high-speed data to their future operations grew by more than 30 percent.

**GROWING IMPORTANCE OF VIDEO**

In light of the increasing importance of video in public safety operations – exemplified by the identification of the Boston Marathon bombers – the study asked respondents about their current and planned use of video. Not surprisingly, more than half of respondents noted that they currently use video solutions, including well over a quarter that are using mobile in-vehicle and/or wearable camera systems.

**ESCALATING THREATS TO SECURITY**

With the seemingly ever-increasing instances of security threats to government and public safety communications networks, the study also asked a number of security-oriented questions. Clearly, the industry is concerned about security breaches. Fully 64 percent of respondents felt their agency communications networks were at least somewhat vulnerable to cyber attacks. Only 12 percent believed their systems were not at all vulnerable to security breaches.

**DEVICE PROLIFERATION**

The survey provided updated information on the types of devices currently being used, or projected for use by first responders and other government workers. Not surprisingly, close to half of respondents said that their first responders use a mobile or smartphone on the job, whether the first responder’s own personal phone or a unit issued by the department. Since “bring your own device” (BYOD) is a major issue for a wide range of agencies, the study somewhat surprisingly showed that less than a third of agencies actually had a BYOD policy in place.
WHITE PAPER
STUDY REVEALS GROWING DEMAND FOR HIGH-SPEED DATA COMMUNICATIONS

THE FUTURE OF PUBLIC SAFETY COMMUNICATIONS
INCREASED EMPHASIS ON MOBILE BROADBAND FOR DATA COMMUNICATIONS

When asked to predict the most urgent future needs for their public safety agencies, 43 percent of respondents mentioned interoperable communications and high-speed data access; another 18 percent indicated that they would rely on mobile data communications as often as voice communications. Possibly driven by the work that FirstNet is doing to develop a nationwide public safety broadband network, study participants indicated a strong interest in providing real-time data access in the field. More than 62 percent of respondents acknowledge – and are preparing for – a future in which delivering real-time voice, data and video access to first responders, wherever they are, is mission critical.

<table>
<thead>
<tr>
<th>IN THE FUTURE, MY AGENCY NEEDS…</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>To easily communicate with agencies in the surrounding area, as well as with federal agencies</td>
<td>23%</td>
</tr>
<tr>
<td>High-speed data access in the field so that we can quickly get the information we need</td>
<td>20%</td>
</tr>
<tr>
<td>To rely on mobile data applications as often as we rely on voice communications</td>
<td>18%</td>
</tr>
<tr>
<td>Dispatch functionality for CAD and radio from the same dispatch workstation</td>
<td>15%</td>
</tr>
<tr>
<td>Local and national database access both in the field and in our primary locations</td>
<td>14%</td>
</tr>
<tr>
<td>Video surveillance systems to increase the eyes on the street and support field personnel</td>
<td>10%</td>
</tr>
</tbody>
</table>

SCENARIO 1: PUBLIC DISTURBANCE
Two police officers respond to a public disturbance call at a notorious bar. As they arrive, the officers find themselves in the midst of a violent fight involving numerous individuals. Immediately calling for backup, the officers wade in and manage to break up the fight before there are serious injuries. As they interview suspects, one of the instigators has no valid identification and appears to be providing a false name. The individual does, however, have a distinctive facial tattoo. On a handheld computer, one officer accesses county criminal records, which also features a database of known tattoos. Getting a match, the officers find the suspect’s real name and discover that he has four outstanding warrants, including one for attempted murder. He is immediately taken into custody and off the streets.
HIGH-SPEED DATA IS BECOMING A TRUE PRIORITY
DATA VIEWED AS MISSION CRITICAL AS VOICE COMMUNICATIONS

For first responders, enhanced situational awareness through immediate access to information – live streaming video of incident scenes, current building schematics, location histories, criminal records and more – is key to increasing public safety efficiency, effectiveness and above all, safety. For first responders in the field, real-time data communications are becoming as crucial as voice communications. In the survey, almost 45 percent of respondents believe that getting data messages through is equal in priority to getting voice messages through. And more than 90 percent believe that data messages are important. First responder expectations are also high. Only 12 percent of respondents said that their first responders do not expect data access to be available during an incident.

REAL-TIME DATA FOR 9-1-1 CALL CENTERS
TECHNOLOGY IS CHANGING HOW MISSION CRITICAL INFORMATION IS COLLECTED FROM THE PUBLIC

There is no question that mobile broadband and the rise of the smartphone are beginning to impact emergency Public Safety Access Point (PSAP) and dispatch operations. More than 56% of American adults have an Internet-enabled smartphone¹ and many use them for applications like text messaging, taking and sharing photographs and capturing video. With research indicating that more than 70 percent of public safety agencies want the ability to use text messages and video from citizens, and 60 percent reporting that citizen-generated data has helped support response,² these particular applications have important implications for public safety. According to 2013 Motorola survey respondents, public safety agencies are in the beginning stages of being able to receive and make use of this data to improve situational awareness, and community and first responder safety.

¹ http://pewinternet.org/Commentary/2012/February/Pew-Internet-Mobile.aspx
² Motorola Government and Public Safety Data Communication Survey, January-February 2012
Participants in Motorola’s 2013 survey make it clear that providing real-time data communications to first responders in the field is a top priority for virtually every public safety agency or department. Responding to questions about the types of devices currently being used to provide access to this important data, almost 80 percent noted they are using intelligent Internet-enabled devices such as smartphones, tablets, laptops and vehicle-mounted computers. When asked the major question of who is providing these smart devices – are they agency-supplied or Bring Your Own Device (BYOD) – responses show that close to half of first responders now use their own personal devices for work-related activities. They also show that more than 62 percent of agencies have no formal BYOD policy, and that of those that do have one, more than half specifically prohibit BYOD. Clearly, this is a practice that is still evolving.

What types of data devices do you, or your first responders, use on the job?

- **26%** Smartphone
- **23%** Mobile phone
- **20%** Laptop
- **17%** In-vehicle workstation
- **9%** Tablet
- **5%** Handheld rugged device

Who provides your first responders with a smartphone/tablet?

- **47%** My first responders use a personal smartphone on the job
- **27%** My agency provides smartphones for command staff
- **21%** My first responders do not use smartphones
- **5%** My agency provides smartphones for all first responders

What is your agency’s policy toward “Bring Your Own Device” (BYOD)?

- **63%** No formal policy
- **15%** Policy permits BYOD
- **18%** Policy prohibits BYOD
- **4%** We plan on implementing a policy this year
The study confirms that video is fast becoming one of the most effective sources of information for public safety operations. Almost 58 percent of respondents indicated that their agencies use video solutions in some combination of fixed, mobile and in-vehicle video applications. The use of real-time video is also on the radar of many agencies. Although only about seven percent of respondents indicated they can currently send live video from in-vehicle camera systems, almost 30 percent said that they would definitely or probably implement streaming video in the next three years. The use of wearable cameras for incident documentation and first responder protection is also beginning to come into use, with more than 30 percent of respondents saying they either currently use, or are considering using, wearable video solutions.

### DOES YOUR AGENCY UTILIZE VIDEO SOLUTIONS?

- **43%**
  - **My agency does not utilize video solutions**
- **25%**
  - **My agency has a fixed video surveillance system**
- **27%**
  - **My agency uses mobile, in-vehicle camera systems**
- **5%**
  - **My agency uses wearable cameras**

### SCENARIO 2: WAREHOUSE FIRE

A passerby notifies a city’s 9-1-1 center that flames are shooting out of the top floor of a large furniture manufacturing plant and warehouse building. As units are dispatched to the scene, first responders are able to view live video of the building from a number of street surveillance cameras, providing them with a real-time view of the scene as they approach. In addition, dispatch sends current building plans that show crucial locations, including hazardous chemical storage areas. The initial units arriving concentrate on keeping the blaze away from the chemicals. Other units use building plans detailing stairway locations and designated escape routes to escort employees on the upper floors to safety. The fire is contained to the premises, and is brought under control with only minor injuries, and with much of the company’s inventory preserved.
PUBLIC SAFETY NETWORKS VULNERABLE
SHARP INCREASES IN CYBER ATTACKS ON GOVERNMENT AGENCIES

In the past six years, the number of cybersecurity incidents reported by government agencies has increased by nearly 680 percent. Cyber attacks are on the rise, and public safety agencies are increasingly coming under attack by hackers whose intentions are not just to steal information, but to disrupt or even totally shut down public safety networks. The reality is, the BYOD phenomenon can exacerbate the situation by exposing government systems to private system vulnerabilities. Respondents are very aware of this threat. Well over 60 percent of respondents indicated that they believe their networks are at least somewhat vulnerable to these attacks, and almost 50 percent are at least somewhat likely to be implementing new security measures – such as practices that establish concentric rings of protection for people, policy, process and technology – in the next year.

IN YOUR OPINION, HOW VULNERABLE ARE YOUR PUBLIC SAFETY VOICE AND DATA NETWORKS TO SECURITY THREATS?

<table>
<thead>
<tr>
<th>Vulnerability Level</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Not Vulnerable</td>
<td>12%</td>
</tr>
<tr>
<td>Somewhat Vulnerable</td>
<td>38%</td>
</tr>
<tr>
<td>Vulnerable</td>
<td>18%</td>
</tr>
<tr>
<td>Very Vulnerable</td>
<td>9%</td>
</tr>
<tr>
<td>Don’t Know</td>
<td>23%</td>
</tr>
</tbody>
</table>

OVER 60% OF GOVERNMENT AGENCIES BELIEVE THEIR NETWORKS ARE VULNERABLE TO ATTACKS

SCENARIO 3: NETWORK INTRUSION

In the early hours of a morning, a cyber criminal hacks into a police network. Few things are potentially more disruptive for public safety agencies than dealing with a network intrusion. Whatever the hacker’s intentions, you can be sure they are not good. Knowing that malware attacks are exploding and manually detecting an intrusion can be difficult and time consuming, the police department has already implemented powerful intrusion detection to protect networks and information. The system not only immediately detects the hacker’s device, but automatically removes it from the network before any damage can be done.

When considering challenges to achieving their public safety communications vision, almost 70 percent of survey respondents identified budget as their primary challenge, while 11 percent noted lack of resources and technical support. Another 10 percent of survey participants identified building consensus with surrounding agencies as a challenge.

### Key Challenges for Next Generation Communications Networks

Budget issues lead the list of challenges to implementing new technology.

**What is your agency’s primary challenge to achieving its next generation communication operations vision?**

- **68%** Budget
- **11%** Lack of resources and/or technical support
- **10%** Consensus with surrounding agencies
- **5%** These technologies aren’t readily available to us
- **3%** Support from the local community
- **3%** System security
- **1%** We don’t need new technology

**Scenario 4: False Complaint Withdrawn**

As an officer turns on his lights and sirens to pull over a driver for speeding and an expired license plate, his dashboard and wearable cameras automatically start recording video. Using his in-vehicle computer, he runs the plate through the county database and discovers that the car has been reported stolen. The officer calls for backup, and as it arrives, the driver begins to run away. After a short chase, the officer corrals the suspect and takes him into custody. At the station, the suspect claims abuse by the officer. Although the entire incident was out of range of the in-vehicle camera, the wearable camera video confirms that there was no abuse, and the suspect withdraws his complaint and is quickly booked.
Study results reveal that the use of data communications continues to trend at a rapidly increasing pace, underscoring the mission critical importance of real-time data communications for first responders in the field. Respondents also provided new information on the proliferation of video as a mission critical public safety tool, with almost 60 percent of respondents reporting the use of video solutions. In addition, they acknowledged the growing threat of cyber attacks on public safety and other government networks, with almost half reporting they are at least somewhat likely to add additional security in the next year.

Against the backdrop of the establishment of the FirstNet nationwide public safety broadband network, the 2013 Motorola Public Safety Industry Study establishes that there are both significant opportunities to take advantage of and significant communications issues that must be addressed. The need to provide first responders with high-speed data and voice communications in the field is seen as paramount. The survey also noted the increasing importance of multimedia, including the streaming of live video to and from the field and the ability of 9-1-1 centers to accept text messages, photographs and video. In addition, certain important policy decisions often remain to be made, especially those dealing with two essential issues: BYOD and network security.

**WHO RESPONDED TO THE SURVEY?** The survey captured responses from a cross section of government professionals, with more than 40 percent coming from chiefs, deputy chiefs and first responders.

**AGENCY SIZE BREAKDOWN:** Survey respondents including public safety professionals from departments and agencies of varying strengths and sizes.

<table>
<thead>
<tr>
<th>Employee Size</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>50 Employees or less</td>
<td>49%</td>
</tr>
<tr>
<td>51-100 Employees</td>
<td>17%</td>
</tr>
<tr>
<td>101-250 Employees</td>
<td>14%</td>
</tr>
<tr>
<td>251-750 Employees</td>
<td>8%</td>
</tr>
<tr>
<td>Over 750 Employees</td>
<td>12%</td>
</tr>
</tbody>
</table>

With responses from more than 850 public safety professionals, Motorola’s 2013 study offers a timely snapshot of the current state of public safety communications technology. The latest in our ongoing series examining the use of next generation technology in public safety, the 2013 study was conducted in February and March, following up on similar research fielded last year. Responses were collected from a wide variety of professionals, with more than 30 percent coming from chiefs and deputy chiefs. Others surveyed included department heads, managers, IT directors, police officers, firefighters, EMS and other public safety users and decision makers.

The 2013 study is part of an ongoing Motorola research initiative to help identify and report on trends affecting communications technology in the public safety industry. For more information on planning and deploying a next generation public safety technology solution, talk with your Motorola representative or visit us on the Web at motorolasolutions.com/nextgen.