Using Future Broadband Communications Technologies to Strengthen Law Enforcement

Appendixes A and B

John S. Hollywood, Dulani Woods, Andrew Lauland, Sean E. Goodison, Thomas J. Wilson, Brian A. Jackson

For more information on this publication, visit www.rand.org/t/RR1462

Published by the RAND Corporation, Santa Monica, Calif.

APPENDIX A: TABLE OF NEEDS FROM THE WORKSHOP

Table A.1 shows the complete list of needs from the Broadband Communications Workshop, sorted by category. Within categories, needs are shown in priority order, with needs with the greatest expected value scores presented first. Each need includes an operational problem ("Problem") and a corresponding specific need to develop and field a potential solution ("Need"). Note that some operational problems are addressed by multiple specific needs, meaning that some problem descriptions are repeated multiple times. The table also shows which tier the need is in (1 = high, 2 = medium, 3 = low). Except for copyediting, all problems and needs descriptions are exactly as they were presented at the workshop.

Table A.1. Prioritized Needs from the Broadband Communications Workshop

Problem	Need	
Guidance on Managing Future Broadband Networks		
Problem: law enforcement is likely going to be hybrid networks combining commercial and FirstNet and existing infrastructure.	Need to provide agencies with guidance on how to acquire, manage, and use mixtures of communications networks: wired + commercial bandwidth + FirstNet + existing infrastructure.	1
Problem: Assumption is that FirstNet devices will (1) be able to log on to FirstNet domain using a set of communications and security standards (LTE -> 5G, Band 14, etc.), and (2) auto-populate with available services and data for that area/jurisdiction/mission at start-up—but what that means operationally is largely to be determined.	Need to develop concepts, policy, and procedures for mutual aid networks in a post land-mobile-radio/FirstNet/broadband era. Need to define the common roles, responsibilities, associated services, information needs, and log-on (authentication and granted permission) capabilities.	1
Problem: In general, what should the public safety network look like in the future? How should information in general be provided, to whom, and for what purposes? What apps/functionalities do we want to put on officers' devices?	Need to coordinate and integrate operational architecture components being developed (who needs what information, with what attributes) by a number of groups (National Public Safety Telecommunications Council, FirstNet, Global, etc.). Can be built as a layered model with core services (e.g., VoIP) to provide with others that can be tailored/deprioritized as needed. Part of this will be conducting an assessment of what data-using functions are most promising to put on devices and what core FirstNet/other services should be available by default. Need to include concepts, policy, and procedures for mutual aid networks. Must explicitly consider data management, legal, and privacy concerns.	1
Problem: Scale of data being collected/exchanged expected to increase dramatically.	Need to look at how data center/cloud models would work in future network topologies and when, in principle, data centers will need to handle huge amounts of data and may have scalability issues.	1
Problem: Criminal justice community needs realistic expectations of what it will get and can actually do on FirstNet and other major broadband networks.	Need to translate bandwidth available on FirstNet and other nets to operational use cases/simultaneous volume in easy-to-understand forms for law enforcement.	2
Problem: Topology of urban networks is changing—will have big implications for how public safety/law enforcement networks will work.	Need to explore implications of how commercial networks are evolving—heterogeneous small cells with overarching coverage in sparser areas. As an example, need to explore combinations of small cells/underlying wired infrastructure to replace towers in dense areas.	2
Problem: Commercially based networks may not deliver needed quality of service and have not been robust to major crises (e.g., Boston Marathon bombing).	Need to develop common sets of service-level agreements that specify what commercial vendors must provide. Need to work with commercial providers to develop mechanisms to provide guaranteed communications and prioritize service for public safety during major events.	3

Table A.1—Continued

Problem	Need	
Problem: Public safety lifecycle of implementation and backward compatibility requirements have to change to make it possible for innovation to happen—currently, public safety implements only after a great deal of validation, etc. But how to square that with the fact that these are life-safety-dependent technologies?	Need to develop new approaches for implementation that allow faster lifecycle implementations of new technologies—more of a model of demonstration and beta testing than "procurement and deployment."	3
Problem: Broadband runs in the background—real-world impact is difficult to measure. Investment decisions and day-to-day allocation decisions need to reflect the value of providing data under different conditions.	Need to identify suitable measures to assess broadband's impacts and cost-effectiveness. Need data to quantify the actual effects on outcomes of interventions that are implemented—i.e., we put a system in place, did outcomes make it better? With these, then need research to precisely assess value of data in different roles and at different latencies. This will inform not just investment decisions but also dynamic network management rules.	3
Problem: Public safety agencies have gotten deals in the past for unlimited access to bandwidth, but those deals are going away as market demand increases. Dense areas will still have market drivers to build out bandwidth. In cities, bandwidth is built out to the point where it is not worth metering (100x current?), but in rural and suburban areas it will not be (maybe 2x current?).	Need two doctrines for law enforcement broadband—one for areas or situations with bandwidth constraints due to lack of buildout incentives and ones without.	3
Problem: Growing consideration over whether jurisdictions should invest in their own wired/wireless networks.	Need to explore, and provide agencies and jurisdictions with guidance, on whether/when/how building a jurisdiction network is the best option.	3
Problem: Need to improve request for proposal (RFP) processes to address limited knowledge of law enforcement agencies.	Need to develop standard RFP languages and processes for communications purchases.	3
Identity, Credentialing, and Access Management (ICAM)		
Problem: Interoperability of communications systems today still requires a lot of prework—very different from the computer world, where third parties can authenticate any device. Need for devices that can connect to many things.	Need new models for general authentication of devices onto a network, more like the DNS in computing. Design devices with multiple input/output options, need intelligence in the network (FirstNet as "router") that finds the resource that the device needs to do what it wants to do (one element of 5G is a requirement to allow any device to connect to any network that it is not forbidden to connect with at any time, and there are devices now that default to open WiFi for carrying calls).	1
Problem: User authentication on new devices becomes more important as the network delivers more access and capability.	Need better ways to do user authentication—make it easy for individual users, such that, for example, if a public safety officer leaves their device behind it is locked, but also accessible by individuals from other agencies.	1
Problem: There are three identities—the device, the person holding it, and the agency that stands behind it—need a way to do that. Currently, no one is directly taking on that problem.	Need to solve the federated identity management problem to allow authentication of one public safety person with a device to connect to a different network—navigating the challenges posed by local control. Requires a governance model that can make these decisions and take on the education task of getting the message out to the individual departments. Need to develop an equivalent of a certificate authority for authentication for public safety communications—FirstNet will have to solve this problem eventually (i.e., you should be able to use your FirstNet device at a major incident in another state).	1

Table A.1—Continued

Problem	Need	
Problem: ICAM for data itself is key—cannot have a different app for every event.	Need research on better schemes for labeling data for access/use in accordance with users' roles and accesses.	2
Prioritizing Information		
Problem: Officers in the field need more-relevant information pushed to them, while minimizing information overload.	Need research on smart software agents for officers in the field to help them get information they need while avoiding information overload.	1
Problem: PSAP personnel are already overloaded—now talking about adding additional data (photos, video, text, etc.).	Need to develop processes (including training/staffing), automation filtering and tools, and procedures to help PSAP employees prioritize incoming data and use data to support operations/avoid information overload.	1
Problem: PSAP and operations center personnel are already overloaded—now talking about adding additional data (photos, video, text, etc.). What if 10 different people send in video of the same shooting? How can the center manage those streams to use them effectively?	Need to develop core algorithms that can filter and prioritize core types of data coming into PSAPs and operations centers and provide useful products to the field. Need to explore leveraging analytics from the carriers to identify incidents of high interest. Would involve creating archives of PSAP data/footage that can be used by researchers to train algorithms. One is for immediate real-time data and one is for reference information that police might find useful later.	1
Problem: Improve agencies' ability to transmit key instructions to the public (emergency instructions).	Need to explore projected communications/social media tools and interfaces with police to see how police might more quickly and completely transmit instructions to selected members of the public and then get key reporting data back. Should include reviewing lessons learned from police use of public reporting apps to date.	2
Problem: Currently video data isn't searchable—it is passive, driven by "human search" watching it.	Need to build intelligence into the video source to limit the amount of video that has to be transmitted/shared, reducing the order of magnitude of video data.	2
Problem: Problem focusing on hierarchical model of information going "from the center" to the field.	Need for tools that enable transmission of information from officer to officer (police department to police department, police department to fire department, etc.) that enable officers in the field to make their own decisions based on the data they receive.	2
Problem: Even though high-definition video stresses network, it is sometimes necessary for evidence.	Need capabilities in the network to know how to cache a high-quality version locally and send a low-resolution version.	2
Problem: Have ability to stream some video from body-worn and other cameras, but capacity is very limited.	Need to develop business rules/procedures to determine when and how real-time streaming of field camera video should occur.	2
Problem: (1) Device displays can "blind" drivers or otherwise distract them from driving, especially at night. (2) Want to get to real-time communications between operators and public ("Can you take a more detailed picture of the suspect?"). (3) Should information be provided differently in response to an officer's fatigue and stress level, given future biometrics tracking of officers?	Need research on how to design device displays that minimize "blinding" effects and other distractions. To consider: In the future, may have augmented reality/heads-up displays as well as other sensors that can detect threats while driving. Should also account for self-driving police cars. Requires standardization of data interchanges between systems, departments, and other sources. Might leverage lessons from commercial gaming and social media development, which also face distraction-minimizing problems. Need research on how to best present information in response to physical condition, especially when fatigued or stressed.	3
Problem: Understanding how you manage a network that has a hierarchical scheme for traffic priority is challenging—since assumption of standard networks is fairness.	Need for work to understand how to do that prioritization, etc., without breaking commercial off-the-shelf systems—whether that is network operations centers (NOCs) and displays or algorithms that can replace the need for the NOCs. How much can you automate?	3

Table A.1—Continued

Problem	Need	
Communications Infrastructure		
Problem: UASs working as communications devices (communications relays), especially as power-tethered UASs.	Need to explore the use of tethered UASs to support rural communications and other areas that need additional communications.	1
Problem: Need to rely on fiber/wired networks when possible to reduce demand on wireless spectrum.	Need to ensure that public safety has access to wired broadband at key sites (PSAPs, operations centers, etc.) in rural areas.	2
Problem: Landline/wired Internet providers—telecommunications, commercial, and government—not really part of public safety network buildout discussion to date.	Need to engage landline/fiber providers in assisting with building out law enforcement/public safety networks.	3
Problem: Tropospheric communications can provide long-range communications into disaster areas without having to fly/float infrastructure into the area.	Need to look at return on investment of tropospheric communications to get connectivity over hundreds of miles into disaster areas. Tropospheric communication addresses the latency issues with some satellite systems as well as access/cost issues. Major disasters have had instances where available satellite communications were overloaded and capacity was unavailable.	3
Network Management		
Problem: Law enforcement is likely going to be using hybrid networks combining commercial and FirstNet and existing infrastructure.	Need research on tools and methods on managing hybrid networks that include wired, commercial broadband, FirstNet, and existing infrastructure components.	1
Problem: Need to decide on priorities for spectrum and specific communications. Need to describe policies for dynamically preempting/getting bandwidth. Current cell downlink maximum for Band 14 is around 7.5 Mbit/sec.	Need to leverage FirstNet work on prioritization and spectrum management to develop a common set of policies and enabling mechanisms for prioritization and spectrum management.	1
Problem: There are growing opportunities to use best available path algorithms, whether over a "broadband network" or to access an IP point of presence directly.	Need to explore use of dynamic routing mechanisms and tools that will allow devices to pick best available connection points and routes, accounting for user needs, available links, and spectrum and capacity availability.	1
Problem: PSAP personnel are already overloaded—now talking about adding additional data (photos, video, text, etc.).	Need to explore load-balancing/cross-agency models for PSAPs and operations centers that provide for maintenance of local knowledge and quality, tailored services.	1
Problem: Desire to manage in-field devices remotely.	Need to leverage new mobile device management technologies to manage devices over the air.	2
Problem: Currently, communications officers for incident command have spreadsheets of spectrum allocations at best.	Need to explore tools to help communications officers during incident command, including spectrum analysis and software defined radio tools.	2
Problem: How do we ensure equal access among users to the logic that determines what data gets filtered out and what gets passed on?	Need research on how to give users equal access to filtering/prioritization logic to ensure that key information is passed on while avoiding saturating the network or causing information overload.	3
Problem: If there is a proliferation of apps on public safety FirstNet, have to think about preemption among apps—i.e., some types of video apps shouldn't preempt while other communication apps should. Distinction of public safety vs. non–public safety will break down.	Need better ways of doing prioritization, and encryption of traffic may make prioritization difficult (or impossible) to implement.	3

Table A.1—Continued

Problem	Need	
Personnel Development		
Problem: Huge demands on both physical storage and human management of data, including redaction of bystanders/victims in video (currently a manual process).	Need to develop roles for people who specialize in data management of video and other high-volume law enforcement data.	1
Problem: Communications is migrating toward services architectures rather than dedicated networks. Setup and maintenance activities are changing.	Need to explore what new "communications services" staff or revised training for existing IT staff will be needed to address future communications architectures. Need to develop new role descriptions and duties, staffing and training concepts for future PSAP/operations center operations.	1
Problem: PSAP personnel are already overloaded—now talking about adding additional data (photos, video, text, etc.).	Need to develop concept of "information flow manager" for PSAPs/operations centers.	2
Problem: Lack of ability to get technical expertise into law enforcement in general.	Need to identify a dedicated cadre of experts who can act as agents for agencies in helping manage law enforcement communications/IT acquisition and maintenance.	3
Problem: Based on present communications systems, operationally, agencies have to keep every officer from talking to each other to avoid overloading both the network and human communications capacities.	Cultural changes will be required in departments, informed by operational analyses to get to a model where extensive peer-to-peer communication among officers is workable.	3
Policy		
Problem: Datacasting/TV white space offer some of the best spectrum for broadband—but how can FCC allocate spectrum to give law enforcement what it will need for a major rise in broadband, beyond FirstNet's allocation?	Need to explore use of datacasting/TV white space and other nontraditional spectrum/bandwidth/capacity for public safety use. Need to explore specific uses of white space, such as time-tolerant backhaul communications. Need to specifically consider use of white space spectrum for rural communications.	2
Problem: Advanced standards for public safety, including multicast, push-to-talk, command-and-control groups, and dedicated spectrum and cells, need to be in forthcoming standards like 5G.	Need to ensure future standards include key law enforcement command-and-control provisions, such as push-to-talk and command-and-control groups.	2
Problem: There is a contradiction between the value of the spectrum that is available to sell to new entrants to the market vs. the capability of ruthless preemption by public safety and perception that law enforcement will consume more and more bandwidth.	If there is a goal to maximize the value of the spectrum, then need to develop incentives for public safety to minimize use of the spectrum (e.g., get onto wired network as quickly as possible, limit use of wireless devices, etc.)—and there is a cross-service coordination issue (e.g., if police department conserves spectrum it doesn't matter if fire department uses it up).	2
Problem: Solutions dependent on commercial infrastructure may not be hardened to public safety grade.	Need to explore models of using portions of public safety communications infrastructure that are not just commercial—and can therefore be hardened to meet public safety grade with public funds. Are seeing more public investments (e.g., areas investing in towers or WiFi for their citizens) where a modest additional investment could harden that element and make it usable as a portion of FirstNet.	2
Problem: State and local agencies are unable to get spectrum that is going unused, notably in rural areas.	Need to explore ways for state and local agencies to get additional spectrum from FCC/federal agencies in areas where it is otherwise going unused. This is in part an FCC issue and in part a need to strengthen federal agencies' mutual aid commitments.	3

Table A.1—Continued

Problem	Need	
Problem: Explosion of IP capacity and PSAPs being built—but most of those may be secured against external (including public safety use) by default.	Need to explore policies/procedures that would consider conditions that would allow public safety responders to get access to normally inaccessible IP PSAPs. Creation of LTE "small cells" that blend characteristics of cell towers and IP points may be one potential solution.	3
Problem: There is a contradiction between the value of the spectrum that is available to sell to new entrants to the market vs. the capability of ruthless preemption by public safety and perception that law enforcement will consume more and more bandwidth.	Need to look at the issue of what level of preemption, probability of preemption, etc. devalues the asset to the level that it calls into question the business model of shared spectrum.	3
Problem: Solutions dependent on commercial infrastructure will never be hardened to the point where they can handle any major event.	Need to define interagency capability delivery and associated governance structure (federal-state-local) to provide capability when needed (i.e., Department of Defense providing emergency satellite capability via FirstNet)—but have to decide how much you are going to back up (voice? voice plus some data?).	3
Problem: Public safety market will never be enough to do customization outside of the $5,000 per device model of development/procurement. Any variance between what public safety wants and the standard that currently exists will cost money.	Need to explore nonmonetary incentives that the federal government can provide to the private sector to incentivize developing technologies to better meet public safety needs (e.g., building or site access, etc.)?	3
Problem: Major policy issues remain before FirstNet can realize the technology capabilities it is supposed to deliver.	Need for standardization of the systems, policies, and processes that will have to be part of/interact with FirstNet—which is counter to the local control model in U.S. public safety. Capabilities that are built into Next-Generation 911 are starting to push the cultural changes associated with this need (e.g., if 911 Center A is transferring calls to B, they will both have to do things similarly).	3
Problem: Have a wide range of standards for different functions, communities, levels and purposes.	Need to review communications and security standards systematically, identify which ones should be implemented, and work to get them implemented nationwide.	3
Problem: Need to improve public safety knowledge about IP networks, LTE, and future communications technologies. This is an ongoing problem. Information and expertise is lacking in many cases in the public safety community. This creates opportunity for vendors to mislead practitioners. These improvements should lead to improved RFP processes.	Need to further explore regional subscription solutions to broadband communications in addition to commercial contracts, in which a government consortium provides communications services for agencies and defines which devices are permitted.	3
Problem: Policy examples—how do we adjudicate between an officer who claims a body camera failed and a vendor who claimed it didn't?	Need to develop common policies for collecting and using data in the field, as well as common provisions for adjudicating them.	3
Technical Research and Development		
Problem: Antennas are consistently an afterthought.	Need antenna research to extend battery life, reduce interference, improve spectrum efficiency, improve throughput, and reduce size/improve form factors. Technologies include physical design, self-tuning, integration into wearables/other form factors. Also need to consider smart controllers for antennas (part of smart radios).	1
Problem: Huge demands on both physical storage and human management of data, including redaction of bystanders/victims in video (currently a manual process).	Need better analytics that automate much of the redaction work.	1

Table A.1—Continued

Problem	Need	
Problem: Solutions available that can allow private sector to share data with police (e.g., security data, camera footage). In the future, will a smart building be able to notify police when it's being broken into? What data should be shared with law enforcement?	Need to develop two public safety–Internet of Things interfaces: one for initial incident reporting, one for communications with responders during events.	2
Problem: Will always need communication needs in buildings and underground—question whether that need will preserve LMR existence, or whether economics will drive LMR out of existence, justifying the investments needed for communication with other wireless technologies.	Need innovations to build the capabilities into other systems that do what LMR currently does (similar to the transition from analog to digital radio previously) to enable phase-out of LMRs (which will free up spectrum that is valuable for other technologies)—flexible "handsets" that can move from network to network, use different waveforms, etc. could be a path.	2
Problem: Current devices can be too difficult to use in the field. Devices built for consumer purposes may not meet law enforcement needs for size, ruggedness, features, weather, etc.	Need to have devices that officers are willing to take out of the car and use—but that are still big enough to gather and structure data for reporting. Should explore different form factors, including screenless data entry/voice data entry and wearables to help improve usability.	2
Problem: Seeing convergence of LMR and LTE.	Need to explore hybrid LMR/LTE devices and networks that can provide both legacy support and best-of-breed services (for voice/very critical narrow band data versus broadband data).	2
Problem: Requirement for active intervention (vs. passive information delivery) is a challenge—i.e., just trust that officers will ask for the information they want.	Need to develop a concept and operational requirements for passive sensors to detect key events happening to officers and route appropriate information to them and from them (as well as other sensors in the area).	3
Problem: Users hampered by split-tunneling restrictions—can't have portals to data sources in different agencies open at once.	Need research on hardware/software/policy issues to deal with split-tunneling.	3
Problem: ICAM is an opportunity to expand and better customize info-sharing networks dynamically.	Need research on new opportunities to share data, especially near-real-time data, such as information about travelers and traveling vehicles or persons who are suddenly having lots of adverse contacts. Needs to consider both political and cost barriers.	3
Problem: Greater capabilities will have larger energy demand, requiring delivery of energy in different ways, better batteries, etc.	Need continued focus on power source technologies for mobile devices that require increasingly more power.	3
Problem: Bring-your-own-device—officers taking photos/videos with their phones, and phones now seized for evidence. (NYPD—officers may not use phones for investigative photos.)	Need to explore development of technical "sleeves" that can make bring-your-own-device/commercial devices compatible and usable on Band 14 secure networks.	3
Problem: Need more study on microcell/personal network waveforms. Using proprietary waveforms across agencies would result in high costs and barriers to interoperability.	Need to explore which waveforms would be most appropriate within microcells (an officer's vehicles, devices) that are very short-range and outside longer-range Band 14 communications. Need to reinforce not using nonstandard waveforms outside of microcells.	3

APPENDIX B: TECHNICAL METHODOLOGY

In this appendix, we provide more detail on how panelists rated the individual needs, how those scores were combined into expected value scores, how the needs were divided into tiers, and how the panelists subsequently were able to vote to move needs into lower or upper tiers.

Rating Questions

Panelists filled out an online questionnaire created using Google Forms to rate each need. Panelists rated each need in response to three criteria on a scale of 1 to 9 (1 low, 9 high). The criteria were as follows:

- How important could this need be in supporting law enforcement?
  - High ratings (7–9) mean that the solution to the need would have a *high impact* on furthering law enforcement objectives where it is used, and would be used *pervasively* across the relevant criminal justice communities. We would assign a 9 to the notable "game-changing law enforcement technologies" in recent years, each of which is associated with a 15–30 percent improvement in performance in a law enforcement outcome where they are used. Examples include the practice of hot spot policing (associated with average crime-reduction effects of over 15 percent in the meta analysis of Braga, Papachristos, and Hureau, 2012) and the use of body armor (could reduce officer fatalities by up to 30 percent—Bir et al., 2011). The 7–9 ratings correspond to needs that, if met, would provide between 70 and 90 percent of a historic game-changing intervention. Using historic benefits of game-changing measures, this roughly corresponds to stating that meeting the need would generate a 10 to 27 percent improvement in a law enforcement outcome where the solution is used. (The maximum score was set at 9, which corresponds to 90 percent—due to inherent uncertainty in the payoff of meeting any need.)
  - Medium ratings (4–6) mean that the need is important to law enforcement—around half the value of a historic "game changing" intervention (40–60 percent).
  - Low ratings (1–3) mean that the need is not that important to law enforcement, estimated to provide at most 10–30 percent of the value of a historic "game-changing" technology.
- Rate the likelihood that this need could be successfully met from a technical perspective, where
  - high ratings (7–9) mean that a path to overcoming technical barriers is clear and seems achievable (70–90 percent chance of success)
  - medium ratings (4–6) mean that technical barriers are difficult and success is uncertain (40–60 percent chance of success)
  - low ratings (1–3) mean that technical barriers are formidable and success requires a breakthrough (10–30 percent chance of success).
- Rate the likelihood that this need could be successfully met from an operational perspective, where
  - high ratings (7–9) mean that a path to overcoming operational and deployment barriers are clear and seems achievable (70–90 percent chance of success)
  - medium ratings (4–6) mean that operational and deployment barriers are difficult and success is uncertain (40–60 percent chance of success)
  - low ratings (1–3) mean that operational and deployment barriers are formidable and success requires a breakthrough (10–30 percent chance of success)
  - here, "operational and deployment barriers" might include problems related to human factors, affordability, maintainability, organizational acceptance, legal/policy (privacy, civil rights, etc.), and security (hacking risks, etc.).

Generating Expected Value Scores

Use of *expected value* is a fundamental approach in decision analysis for assessing the value of options under uncertainty (e.g., de Neufville, 1990, pp. 312–313); it is also the approach used in prior RAND research on criminal justice technology needs, as well as a line of similar research on optimizing science and technology investment decisions.[1]

[1] Hollywood et al., 2015a, 2015b; Jackson et al., 2015; Silberglitt et al., 2015. Prior to these studies, expected values were used in a series of related RAND studies to assess portfolios of investment options (Silberglitt and Sherry, 2002; Chow, Silberglitt, and Hiromoto, 2009; Silberglitt et al., 2004; Landree et al., 2009). In our case, the "investment options" are taking action to address a specific criminal justice technology need.

In this study's context, *expected value* is defined as the importance of the need (measured on a scale from 1 to 9) times the estimated likelihoods that the need could be addressed successfully from both technical and operational perspectives (also on a scale from 1 to 9; as noted, these correspond to a 10–90 percent of chance of success). Specifically, the formula for the expected value score for need i, $E(V_i)$, from any given panelist's ratings is:

$$E(V_i) = V_{il} L_{it} L_{id}$$

Here, V_{it} is the estimated importance of the need to law enforcement, and L_{it} and L_{id} are the probabilities of success from technical and operational perspectives, respectively. The maximum possible expected value score is 9^3, or 729.

To create an overall expected value score for each need, we took the median of all the panelists' individual expected value scores for each need. The median is used as it is robust—it estimates the center of the distribution in a way that is resistant to outliers and atypical distributions. Medians also do not require making any assumptions about the underlying statistical distribution of the scores.

Table B.1 shows descriptive statistics on the averages, over all 68 needs, of the means, standard deviations, medians, and interquartile ranges of the participants' ratings for each need. As shown, the statistics are broadly similar across each of the three input ratings (importance, technical feasibility, and operational feasibility), with central measures for operational feasibility being a bit lower.

The expected value scores do have a real-world interpretation. The expected percentage by which a solution to a given need will improve a key law enforcement outcome in places where the solution is used is:

$$E(\Delta Y_i) = \frac{(22.5 \pm 7.5) \cdot E(V_i)}{1{,}000}$$

The average of all the median expected value scores (351—see Table B.1) corresponds roughly to our panel stating that coming up with a solution for a need would improve a key law enforcement outcome in locations where that solution is used by an average of about 8 percent. In comparison, the top-rated need from the workshop—providing agencies with guidance on how to use hybrid communications networks—had a median score of 501, which translates into about an 11 percent expected improvement. The lowest-rated need from the workshop had a median score of 148, which translates into about a 3 percent expected improvement.

Obviously, it is not the case that the we, or the expert panel, would take these estimates as reliable predictions of what would happen to key law enforcement outcomes if solutions were developed and fielded. Nonetheless, we do believe that this prioritization methodology does provide a reasonable way to calibrate the importance of the needs in a way that makes sense from a real-world perspective—more so than simply asking general questions about how important a need is to law enforcement.

Table B.1. Descriptive Statistics on How the Needs Were Rated, on Average

	Importance	Technical Feasibility	Operational Feasibility	Expected Value Score
Average of the needs' mean ratings (n = 68)	6.79	6.88	6.37	330
Average of the standard deviations of the ratings for each need	2.11	1.90	2.07	218
Average of the median ratings for each need	7.25	7.36	6.65	351
Average of the interquartile ranges of the ratings for each need	2.78	2.81	2.98	326

Subdividing the Needs into Tiers

We used each need's overall expected value to categorize it into one of three tiers. Tier 1 includes the highest priority needs; the discussion and recommendations in this report (and other Priority Criminal Justice Technology Needs Initiative reports) are focused on the Tier 1 needs. Tier 2 includes the medium-priority needs while Tier 3 includes the lowest priority needs.

To subdivide the needs into tiers, we employ *hierarchical clustering*, specifically using Ward's method (Ward, 1963; Murtagh, 1985). Hierarchical clustering is an iterative process. With each iteration, two records and/or two sub-clusters that have minimum "distance" from each other are merged into a larger sub-cluster. The final result is a *dendrogram*, a hierarchical tree that shows exactly when individual records and sub-clusters were merged into larger clusters, with records on the same small branch typically much "closer" than records on branches farther away. To get a few clusters (in our case three clusters corresponding to the three tiers), one simply subdivides records by their largest branch. With Ward's (1963) method for hierarchical clustering, the "distance" is the weighted squared Euclidean distance between the centers of each cluster. (Here, a cluster "center" is the average of all the records in that cluster.)

Hierarchical clustering is one of the principal types of clustering algorithms. It has the advantage that one can see the full hierarchy of when records and sub-clusters were combined (Manning, Raghavan, and Schutz, 2009, p. 377; Frontline Systems, Inc., 2015). For tiering needs, this feature has the advantage that in cases where largest subclusters are not practical for analysis (notably, when the algorithm returns only a few Tier 1 needs or tries to make more than half the needs Tier 1), one can manually review the second-tier subclusters and manually adjust the tiers into more-practical groupings.

For this study, we used the "hclust" package in the R statistical environment, via the Wessa statistical web portal (Wessa, 2012).

Round 2 Voting

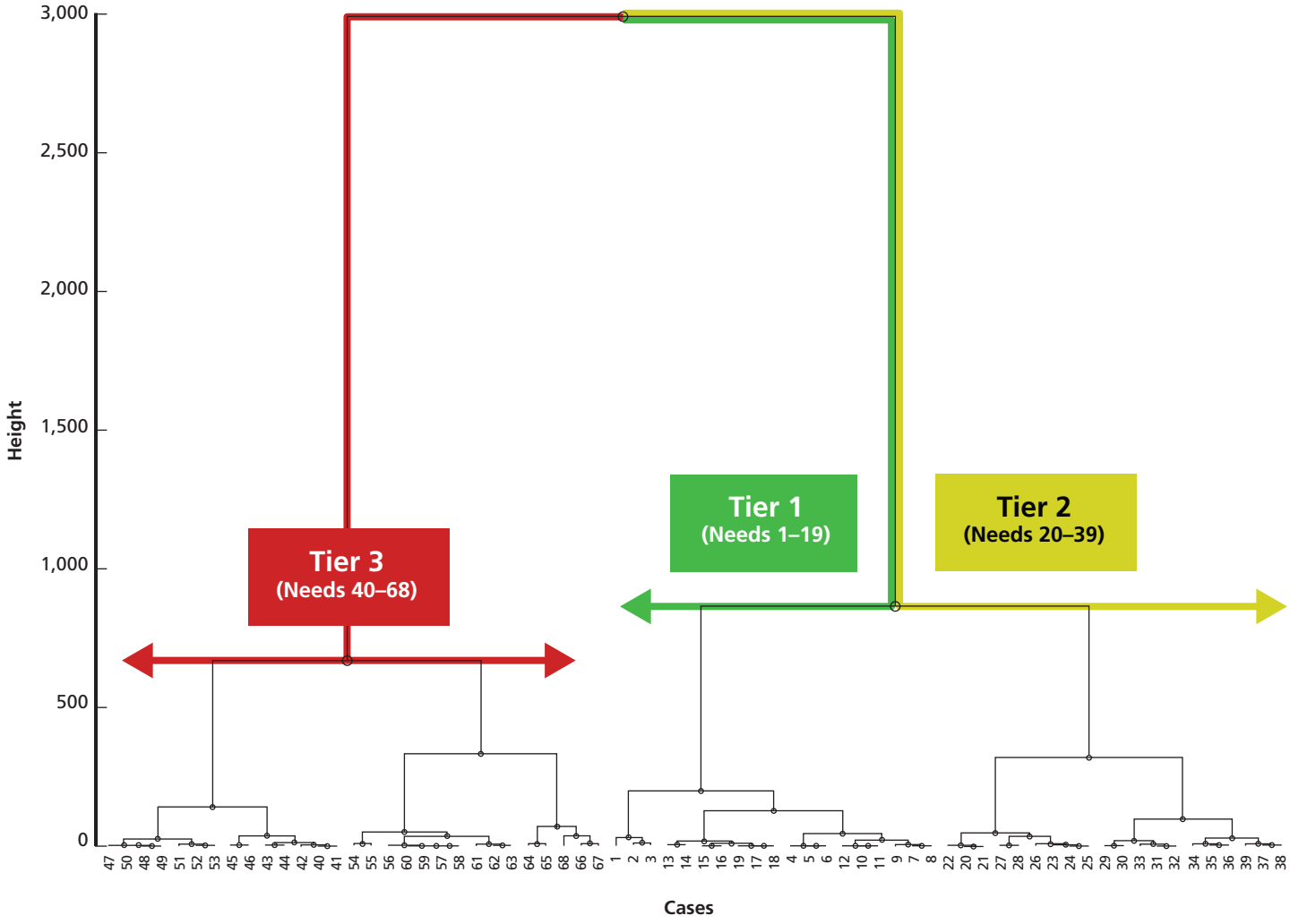
Round 2 of needs prioritization occurred in the weeks following the broadband communications panel. Again, panelists filled out an online questionnaire, this one built using the Qualtrics platform (2015). Panelists had the opportunity to review all the comments provided on the needs during the initial needs ratings, as well as what tier the needs fell into. They then had the opportunity to vote to keep the need in the same tier, promote the need into a higher tier, or demote the need into a lower tier.

The votes had the impact of raising or lowering the needs' overall expected value score. To determine how much each vote meant, we first calculated the range between the highest and lowest expected value scores. We then calculated how much each vote would need to count in order to raise the lowest-ranked need to be the highest-ranked need if every participant clicked the "raise tier" button. In this workshop's case, the range was 387 points, and there were 34 participants who rated needs in Round 1, so each vote adjusted the need's overall expected value score by 11.38 points.

Following the completion of Round 2, we re-tiered the needs using the adjusted overall expected value scores, again using the hierarchical clustering algorithm. Figure B.1 shows the complete dendrogram from hierarchical clustering (returned using Wessa, 2012). The labels on the needs (bottom axis) reflect the rank of each need's adjusted expected value score, so that "1" corresponds to the need with the highest score, "10" corresponds to the need with the tenth highest score, and so on.

The three tiers correspond to the three largest branches on the tree. Thus, Tier 1 corresponds to needs with adjusted scores ranked from 1 to 19, Tier 2 corresponds to needs ranking 20 to 39, and Tier 3 corresponds to needs ranking 40 to 68.

Figure B.1. Final Dendrogram of Need Clusters Following Round 2 Voting



RAND *RR1462-B.1*

APPENDIX B BIBLIOGRAPHY

Bir, C., J. Cecconi, A. Dennis, M. McMullen, and C. Sloane, *Behind the Badge: Management Guidelines for Impacts to Body Armor*, Washington, D.C.: National Institute of Justice, Award Number 2004-IJ-CX-K0402011, February 2011. As of August 9, 2016: https://www.ncjrs.gov/pdffiles1/nij/grants/233645.pdf

Braga, Anthony A., Andrew V. Papachristos, and David M. Hureau, "The Effects of Hot Spots Policing on Crime: An Updated Systematic Review and Meta-Analysis," *Justice Quarterly,* iFirst, 2012, pp. 1–31.

Chow, Brian G., Richard Silberglitt, and Scott Hiromoto, *Toward Affordable Systems: Portfolio Analysis and Management for Army Science and Technology Programs*, Santa Monica, Calif.: RAND Corporation, MG-761-A, 2009. As of August 9, 2016: http://www.rand.org/pubs/monographs/MG761.html

De Neufville, Richard, *Applied Systems Analysis: Engineering Planning and Technology Management*, New York: McGraw-Hill, Inc., 1990.

Frontline Systems, Inc., "Hierarchical Clustering," *Frontline Solvers*, 2015. As of August 9, 2016: http://www.solver.com/xlminer/help/hierarchical-clustering-intro

Hollywood, John S., John E. Boon, Jr., Richard Silberglitt, Brian G. Chow, and Brian A. Jackson, *High-Priority Information Technology Needs for Law Enforcement*, Santa Monica, Calif.: RAND Corporation, RR-737-NIJ, 2015a. As of August 9, 2016: http://www.rand.org/pubs/research_reports/RR737.html

Hollywood, John S., Dulani Woods, Richard Silberglitt, and Brian A. Jackson, *Using Future Internet Technologies to Strengthen Criminal Justice,* Santa Monica, Calif.: RAND Corporation, RR-928-NIJ, 2015b. As of August 9, 2016: http://www.rand.org/pubs/research_reports/RR928.html

Jackson, Brian A., Joe Russo, John S. Hollywood, Dulani Woods, Richard Silberglitt, George B. Drake, John S. Shaffer, Mikhail Zaydman, and Brian G. Chow, *Fostering Innovation in Community and Institutional Corrections: Identifying High-Priority Technology and Other Needs for the U.S. Corrections Sector*, Santa Monica, Calif.: RAND Corporation, RR-820-NIJ, 2015. As of August 9, 2016: http://www.rand.org/pubs/research_reports/RR820.html

Landree, Eric, Richard Silberglitt, Brian G. Chow, Lance Sherry, and Michael S. Tseng, *A Delicate Balance: Portfolio Analysis and Management for Intelligence Information Dissemination Programs*, Santa Monica, Calif.: RAND Corporation, MG-939-NSA, 2009. As of August 9, 2016: http://www.rand.org/pubs/monographs/MG939.html

Manning, Christopher D., Prabhakar Raghavan, and Hinrich Schutze, *Introduction to Information Retrieval* (online edition), Cambridge, UK: Cambridge University Press, 2009. As of August 9, 2016: http://nlp.stanford.edu/IR-book/

Murtagh, F., "Multidimensional Clustering Algorithms," in COMPSTAT Lectures 4, Wuerzburg: Physica-Verlag, 1985.

Qualtrics, LLC, homepage, 2015. As of August 9, 2016: http://www.qualtrics.com/

Silberglitt, Richard, Brian G. Chow, John S. Hollywood, Dulani Woods, Mikhail Zaydman, and Brian A. Jackson, *Visions of Law Enforcement Technology in the Period 2024–2034: Report of the Law Enforcement Futuring Workshop*, Santa Monica, Calif.: RAND Corporation, RR-908-NIJ, 2015. As of August 9, 2016: http://www.rand.org/pubs/research_reports/RR908.html

Silberglitt, Richard, Lance Sherry, Carolyn Wong, Michael S. Tseng, Emile Ettedgui, Aaron Watts, and Geoffrey Stothard, *Portfolio Analysis and Management for Naval Research and Development*, Santa Monica, Calif. RAND Corporation, MG-271-NAVY, 2004. As of August 9, 2016: http://www.rand.org/pubs/monographs/MG271.html

Silberglitt, Richard, and Lance Sherry, *A Decision Framework for Prioritizing Industrial Materials Research and Development*, Santa Monica, Calif.: RAND Corporation, MR-1558-NREL, 2002. As of August 9, 2016: http://www.rand.org/pubs/monograph_reports/MR1558.html

Ward, J. H., Jr., "Hierarchical Grouping to Optimize an Objective Function," *Journal of the American Statistical Association*, Vol. 58, 1963, pp. 236–244.

Wessa, P., "Hierarchical Clustering (v1.0.3)," *Free Statistics Software* (v1.1.23-r7), Office for Research Development and Education, 2012. As of August 9, 2016: http://www.wessa.net/rwasp_hierarchicalclustering.wasp/