WORKING TOGETHER
Partnering To Face Today’s Critical Public Safety Technology Issues

Legislative and Regulatory Needs for NG911
Advanced Cyber Threats
Procurements Made Easier
Partnership and Internal Governance
Contents

Message 3
by iCERT’S Executive Director, George Rice

Procurements Made Easier 4
David Jones

Partnership and Internal Governance 9
Cheryl Giggetts

Legislative and Regulatory Needs for NG911 14
Paul Fahey

Advanced Cyber Threats 17
Patrick Flynn

Closing 23

About the Authors 24

Additional Resources 25
Letter from George Rice, Executive Director

This publication is intended to foster understanding between public and private sector emergency response technologies professionals by providing key points of information on private sector capacities and processes, as public agencies look to engage commercial enterprises in support of emergency calling and communications technology projects. Through this Guide, iCERT member companies propose to inform our public sector colleagues as to how to prospectively define needs, and to work with consultancies and integrators as core components of a successful implementation or upgrade strategy.

The primary audiences for this publication are public agency emergency communications professionals, elected officials, and associations serving these constituencies. Yet, business and government entities alike will acquire key understandings and tools for working together to improve development, procurement, and deployment processes for emergency response technologies. The Guide will add value to the field by providing a clearer setting for emergency communications technology planning and related procurement practices, and thus act as a bridge between the public and private sectors.

As an undergirding principle for effective planning, properly secured resources lead the way. Key to maintaining effective emergency calling and communications systems is a consistent and reliable source of funding. Industry Council members and partners continue to work to ensure that elected and appointed officials know of the critical need for properly resourced emergency calling, and that funds collected and specifically intended to support 911 actually reach local communications centers for service delivery and technology deployment.

Our nation’s public safety professionals make technology investment decisions every day. Available funding resources help guide these decisions as agencies look to improve their systems and ensure effective deployment of emergency services. Absent the requisite resources, no emergency communications agency, center, program, or plan can reach its potential or position itself effectively for the future.

The authors of this Guide—iCERT member company staff volunteers—have shared their insights and experiences throughout the pages that follow. In discussing issues related to Procurement Process Readiness, Funding and Resource Development, Partnerships and Internal Governance, along with Information and Network Security, they have painted a picture of key matters that should be taken into consideration as the planning process begins, and as it runs its course to successful completion.

As communications operations combine into regional centers or shared resource settings, the need for greater data storage and analytics continues to grow, and the current economy continues to compel agencies to do more with fewer resources, the nature and extent of emergency communications planning has transformed into what is now an ever-changing landscape, where many challenges lie ahead for the field of emergency response technologies. This Guide will illuminate some of these challenges by offering concepts for public-private collaboration.

George S. Rice, Jr.
Executive Director, iCERT
There are many situations that get the blood pumping and the adrenaline rushing in public-safety agency managers. Many of them involve lights and sirens. There is one situation, however, that doesn’t involve an emergency of any kind, but still creates feelings of stress, anxiety and even dread: the procurement of a multimillion-dollar emergency communications solution.

There is good reason for the stress, as there is a lot on the line, starting with the dollars that are involved. These are challenging times for many, if not most, public-safety agencies given that tax revenues and grant programs have decreased dramatically over the last decade. The bottom line is there is no money to waste, which means agencies must receive the greatest bang for the buck regarding their system and equipment purchases, and there is little, if any, room for error.

The long amortization periods associated with such procurements are a complicating factor. Amortization cycles can range from one to two decades, which means the agency is going to have to live with its decision for a very long time; when it comes to procurements, there are no do-overs. Now add to all of this the single most important factor—the solution must work flawlessly when lives are on the line, each and every time—and what you get is a task that quickly can become a giant headache for agency managers who often are unprepared for the process.

Public-safety managers have very time-consuming and challenging day jobs, and often don’t have experience in procurement strategy. After all, it’s not every day an agency sets out to purchase a $20 million dollar radio system or a $5 million dollar computer-aided dispatch system.

Sometimes, agencies choose to hire a consultant to lead them through the procurement process. Whether you choose to go that route, this article examines some of the basic strategies to help you end up with a solution that meets your needs and expectations, and fits within your budget.

Define the Requirements

The first step in the process is to get all of the key decision-makers and stakeholders into a room to get their input regarding the new or upgraded system being procured. Stakeholders should comprise all users of the system. Obviously, this will include the municipality’s law enforcement, fire and emergency medical service (EMS) first-responder agencies, but also ancillary departments—such as emergency management, public works and transportation—that provide vital services during and after emergency incidents, and which often are thrust into the role of first responder, depending on circumstances. In these meetings there are no wrong answers or dumb questions.

You need to document what the decision-makers and stakeholders truly think, especially their concerns. Keep in mind that while it is important to gather and understand all of their perspectives, it is equally important to realize there is no way to make everyone happy. In fact, while consensus always should be the goal, most often it is not something that can be realized—there are just too many conflicting opinions. However, this is not a bad thing, for it is through constructive debate that one is able to determine the challenges the agency is facing that necessitate a system upgrade or replacement, and the optimal path for resolving those challenges.

In that regard, the most important takeaway from the meeting(s) with decision-makers and stakeholders is a differentiation between needs and wants. Though this distinction is important to make, it often is difficult to achieve; sometimes a very thin line exists between needs and wants. The ability to make this differentiation lessens the risk that the agency ends up specifying a solution that it cannot afford.
Even more critical are those times when something an agency wants would eliminate competition, which in turn reduces interoperability and/or drives up costs. This should be avoided at all costs. When developing the system’s technical specifications it is crucial to ensure, to the highest possible degree, that all components are manufactured to current and open industry standards.

**Competition among multiple vendors is the only way to ensure the agency receives the best possible solution at the lowest possible cost.**

Once the technical specifications have been identified, it is time to draft a procurement document, which can take many forms, such as a request for proposal (RFP). As with the technical specifications, it is vital the RFP is written so that the mandatory components of the system being procured are completely open to competition, i.e. that they adhere to industry standards, for it is in the agency’s best interest to attract as many vendor proposals as possible.

Sometimes an agency will be tempted to write an RFP in such a way so as to ensure a favorable outcome for a particular vendor. This usually happens when there is a long history and solid comfort level with a vendor. However, this is a bad idea. Competition among multiple vendors is the only way to ensure the agency receives the best possible solution at the lowest possible cost.

**Procure the Solution**

After the RFP is satisfactorily crafted and distributed to the vendor community, the procurement process moves to another level. The very first step in this stage is to invite interested vendors to a pre-bid meeting, which gives them an opportunity to meet the agency’s leadership and to ask questions; the same holds true for the agency. While a key goal of the pre-bid meeting is to establish a comfort level between the vendor and the agency, the more important goal is to answer questions that both sides have because no matter how thorough or well-written the RFP there will be aspects of the project that are unclear or unapparent, particularly to the prospective vendor.

While they can be conducted online via services such as WebEx, it always is recommended that pre-bid meetings be conducted in person for a variety of reasons:

- It usually is easier to reach a comfort level with the other party when everyone is in the same room.
- In-person meetings provide the opportunity to conduct site visits.

While these may not be deemed important when implementing CAD, records management or audiovisual systems, they are vitally important when deploying radio and microwave systems because they allow vendors to see the environment in which they will be working. In particular, site visits provide an opportunity to assess actual installation spaces and other physical factors that might have an adverse effect on system performance or require complex installations. This will help the vendor design and engineer its proposed solution. From the agency’s perspective, the more solid the information a vendor has at its disposal the better; the more assumptions that a vendor has to make, the greater the risk that the proposed solution won’t meet the agency’s needs.

All of that said it is important that the agency makes pre-bid meetings and site visits encouraged, yet optional, because some vendors will balk at them given the time commitment and unreimbursed expenses. Consequently, it is important the agency does not put into place any stipulation that will constrain the number of RFP responses it receives.

Now it is time to evaluate the responses. A critical element in the evaluation process is a scoring matrix, which provides both a qualitative and quantitative method of evaluating proposals. The qualitative aspect involves determining to what degree the vendor’s
A key element of this determination involves gauging the believability of the vendor’s responses...

proposal meets the agency's requirements. There are dozens of items in the RFP to which the prospective vendor will need to express its ability to comply. Each of these items carries a different weight; naturally, needed items carry a much greater weight than wanted items.

A key element of this determination involves gauging the believability of the vendor's responses, and there are numerous factors to consider when doing so. Chief among them is the vendor's previous experience with similar projects, and whether the outcomes were good or bad; regarding any bad outcomes, it is important to also understand how bad, e.g., whether the system was inoperable for any significant time period and/or any litigation ensued as a direct result of the vendor's performance. Other factors include the vendor's financial capabilities and the availability of its resources.
Based on this qualitative analysis, each vendor response will receive a score, and then an aggregate score will be determined—this is the quantitative aspect of the scoring matrix. The aggregate score provides a good tool for comparing the vendor solutions, and is an easy way to rank them.

The scoring matrix must be objective, clearly identify the agency’s expectations, and be understood easily by the agency. The last requirement is particularly important because it is the agency that will perform the evaluations, not the consultant if one has been hired. The consultant plays a key role in helping the agency create the scoring matrix and can assist the agency at times to prevent it from coming to false conclusions based on erroneous assumptions. But make no mistake about it: It is the agency that will evaluate the proposals and ultimately make the selection.

Solution cost should be near the bottom of the list of criteria that an agency must consider. Far more important is whether the solution meets or, ideally, exceeds the agency’s needs and expectations. However, cost must be considered sooner or later, and the agency might find itself in a position where it will need to make a few tradeoffs in order to procure the solution that provides the best value given its budget parameters.

Evaluation and scoring of vendor proposals is all about the agency selecting the vendor that provides the best overall solution. It’s not about awarding the project—that’s the next big hurdle to clear.

In order to award the project, a contract must be negotiated. Earlier this article touched on the importance of avoiding a scenario where only one vendor responds to the RFP; this is important because a sole-source scenario places the agency at a negotiating disadvantage. Simply put, the more competition there is, the more aggressive each vendor will be with its pricing. But there is more to it than that. From the agency’s perspective, itemized pricing is the key to effective contract negotiation; the key components are an itemized equipment list, labor rates and the estimated hours per task. Itemized pricing gives the agency the opportunity to adjust or even eliminate certain items to ensure the project fits within its budget parameters. In a competitive procurement, a vendor is much more likely to provide such pricing.

If several vendor proposals are very close in terms of solution specifications and cost, the agency should consider issuing a “best and final offer” request. The result likely will be that the vendors will attempt to improve their proposals by offering additional considerations or lowering their prices.

Now that the contract has been negotiated and the project awarded, it is time to implement the new or upgraded system.

**Implement the Solution**

The first step is to design the solution. Of course, the vendor doing so must adhere to the agency’s requirements, to industry standards and best practices, and to solid engineering practices. But even when the vendor does all of this, problems can occur.

Let’s consider a radio system deployment. The vendor has decided the optimal way to ensure the system provides the coverage the agency requires is to place X number of antennas on Y number of towers. But while this system design works well from an engineering perspective, it doesn’t work for the agency, because the vendor has failed to consider the impact this design will have on the agency’s tower-lease costs. Consequently, the vendor will need to develop an alternate design that is better balanced. This level of scrutiny must be applied to every aspect of the solution design.

Once the vendor and the agency have agreed on the solution design it is time to install the system. However, if the agency is implementing an LMR system, there is one precursor to installation that must be executed, which is to stage the system. Staging generally is done at the vendor’s facility. While staging usually doesn’t uncover many surprises, it does represent the last opportunity for the agency to make major changes to the solution.
The procurement of a new public-safety communications system is arduous, stressful and complicated—but when done well, the new or upgraded system will provide excellent service to first responders and the citizens they serve and protect for years, even decades, to come.

That’s because once the equipment has been shipped to the agency, it typically has been paid for—which makes it considerably more difficult to execute a substantive change.

Once the system is installed, it needs to be performance tested. This is something the equipment vendor can perform without oversight, but it is strongly recommended that independent subject-matter experts be employed for this task. If the testing is performed by an equipment vendor without oversight the agency would have less recourse if it accepts the results of the vendor’s performance test, should problems occur in the future.

The final step is to put the system through error testing once it has gone live. Error testing typically ensues for a period of 30 to 60 days, and is necessary because no simulation can replicate the system operation when it is handling user traffic under full load.

Here’s an example: A client once implemented a new microwave system, which handled performance testing very well. However, once the system was under full load, one of the network processors couldn’t operate fast enough to handle all of the traffic and eventually overheated, then failed. This link was tested repeatedly during performance testing and passed each and every time. Only under full load did the problem manifest itself. That type of event can happen anywhere in the system, which is why error testing is so important. Performance tests are effective in providing a comfort level that the system will work as designed, but testing the system when it is handling real traffic under full load is the only way to know for sure.

You might be wondering about the wisdom of running live mission-critical traffic over a new or upgraded system before knowing for sure that the system can handle the rigors. Contingency plans take this into account. During the system cutover period, the agency should maintain access to the legacy system, just in case. If a problem were to occur, users would quickly and seamlessly be transferred to the legacy system, which provides a proverbial safety net. Only when the agency is 100 percent sure that the new system is working properly will it decommission the legacy system—until then, the rollback option will be available.

The procurement of a new public-safety communications system is arduous, stressful and complicated—but when done well, the new or upgraded system will provide excellent service to first responders and the citizens they serve and protect for years, even decades, to come.

By heeding the advice, tips, and strategies in this article you put yourself and agency in the best position to be successful. Instead of using your valuable time reacting to poorly managed procurement process you will have reduced stress and keep your focus on the most critical issues and decisions.
Partnerships and Internal Governance

CHERYL GIGGETTS Senior Vice President, Technology Solutions, AECOM

No two public safety agencies are identical. While there are many similarities, each agency has evolved based on its own situation, and there are many unique factors that have contributed to the current state of each agency. Agencies tend to have their own identities and pride in what they do and who they are. While public safety agencies have traditionally partnered on things like regional or specialized task forces or mutual aid agreements, the trend over the past 10 years has been a broadening of areas where partnering is being considered.

Fiscal constraints and the ongoing desire to reduce staffing costs through structural changes to an organization have created interest in new partnership opportunities. These can take on different forms such as a shared services agreement, consolidation of like or similar operations, or external partnering such as a Public Private Partnership. In all cases the two most important factors are fiscal and governance issues.

Changes to operations should only occur by design, and should be carefully considered during planning and implementation. Some changes to operational procedures may be desirable; other changes may be fiscally necessary. All changes should be thoughtfully managed. An important factor in evaluating the merits of a partnership is a focus on making positive improvements to all aspects of the delivery of public safety services.

It is strongly advised to undertake a feasibility study of any contemplated consolidation, shared services agreement or Public Private Partnership (PPP). Such a study should consider issues including: one-time and ongoing costs, cost sharing models, governance models, operational impacts, transition planning issues, merits and challenges and an estimated schedule with key milestones.

Public Private Partnership Discussion: Traditional vs. Non-Traditional Funding Models

Traditional methods of funding large scale public safety technology projects often include the implementation of a Special Purpose Local Option Sales Tax, issuing public bonds to finance the projects or a combination of financing and capitol project funding through the normal budget process.

Non-traditional funding approaches can include a PPP whereby a private sector partner funds all or part of the project in return for a future revenue stream based on user fees or other pay-to-use-models. One potential advantage of a PPP is the shifting of funding responsibility away from the system users to a private system owner or operator. This arrangement may also include the assumption of financial obligations for future system expansions, maintenance and upgrades.

No two public safety agencies are identical. While there are many similarities, each agency has evolved based on its own situation, and there are many unique factors that have contributed to the current state of each agency.

Other financing alternatives to traditional funding can include a lease-to-buy arrangement or financing provided by the system vendor that would then be repaid over time (an alternative to bonding). Many of these scenarios also often shift expenditures for leasing or user fees into annual operating budgets and away from debt service or capital expenditure budgets.
Agreements as to how project costs will be covered vary based on the needs, desires and abilities of the project participants. Some costs such as the system infrastructure can be considered shared costs whereas radio costs might be considered an agency-specific cost. There are many different possibilities to consider when system partners develop a funding model. Once cost element responsibilities are agreed to, the manner of funding each can be accomplished in various ways.

**Functional and Performance Requirements Assurance**
An essential element of any technology system project is ensuring that the system and equipment will meet all of the required functional and performance specifications. A public radio system, for example, must perform reliably and meet the operational needs of the users. Significant thought and effort goes into the development of...
Overall Cost Discussion

There is no particular cost advantage or cost savings involved, but costs can shift from a traditional category into user fees (as one example). The overall cost for equipment and services is going to be similar no matter who buys or owns the system and equipment. Internally, the actual cost to a PPP partner such as an equipment and system supplier may be less than the cost to a customer under a traditional purchase, as the PPP partner could choose to defer what would typically be a profit margin on the project. In the end, their business plan would normally be designed to recover this lost profit margin through future fee structures.

In a similar manner, future costs such as maintenance and upgrades are still real costs and will either need to be paid directly by users or built into user fees. Also, The PPP partner will often need to recover reasonable system administration costs if they have overall responsibility for system performance and operations. Normally this would also include the cost of funds (for them to build the system) and would be included in their business plan model.

Typical Assurances that a PPP Partner Would Require

A PPP partner’s business plan will need to assume an adequate revenue stream over a long enough period of time to recover all costs and to meet return on investment goals. As an example, a radio system project’s costs are typically recovered through user fees. That will almost always include an annual cost per radio and may also include a one-time, buy-in cost. The PPP partner will need to have a contractual guarantee that there will be X number of users paying to use the system for a certain number of years at an established fee.

Using our example of a radio system, user agencies may be required to guarantee a certain number of radios for a period of years at an annual per radio rate of “$X” with a CPI escalator clause. Alternatively they may require an annual composite fee amount of “$Y” as a guaranteed minimum if the number of users were to decline. A PPP can shift initial funding responsibilities to a private partner, however, in the end the users are paying the cost, just in another manner.
Key PPP Success Factors
Any PPP arrangement needs to be structured so that there is value and benefit to both the public and the private partners. Typical elements of this shared value proposition are outlined below:

- The Private Partners need a revenue model that allows them to recover their costs
- The Private Partners will not want to accept responsibility or liability for things that would be beyond their reasonable control
- The Public Partners need assurances that the system and equipment supplied will meet their requirements, be reliable and durable
- The Public Partners need an understandable and predictable cost/fee structure so they can predict budget needs
- The Public Partners need assurances and protections regarding long term system ownership, maintenance and reliability in the event that a Private Partner goes out of business or is acquired by another firm
- Adequate and reasonable system governance and administration agreements need to be established which create a collegial working relationship between the Private and Public Partners

PPP agreements that include the above success factors can prove to be beneficial for all partners, but they take a considerable amount of effort and negotiation to establish.

Governance Model
One of the first issues that must be resolved in a partnership, consolidation or sharing of services is the governance structure. There are a number of models for a partnership, or consolidation. Let us look at how this might work for a consolidation or a shared services model:

- One possibility is for one of the existing agencies to absorb the public safety services of the other participants that are being combined.
- Another would be for one agency to provide the services, with the other agencies contracting for those services.
- The third alternative is an independent entity, where a newly formed department or agency provides public safety services for all of the participating parties.

All of these models would require an Intermutual Agreement (IMA) or contract between the affected parties. Usually, a two-tiered governance structure is established to provide oversight, comprised of an Executive Committee and an Operations Committee.

Executive Committee
The Executive Committee should be comprised of members from the participating parties. One person should be appointed by the party leadership of each entity as a member of the Executive Committee. It is recommended that the appointments be made from senior leadership. The selection, however, would be the individual decision of each participating party. This Committee should be the general policy making authority. Its functions should include:

- Entering into contracts
- Acquiring, holding, or disposing of property
- Approval of an annual budget and expenditures
- Hiring, employing and terminating management staff
- Adopting and revising any bylaws

Operations Committee
The second part of the governance structure is the Operations Committee. The Operations Committee should consist of Subject Matter Experts (SME) of the participating parties. The function of the Operations Committee is to provide guidance and input to the Executive Committee on operational and other appropriate issues. It is envisioned that the Operations Committee would work with the public safety management to develop appropriate standards and procedures concerning performance, personnel selection and training, and other technical and operational issues as directed by the Executive Committee.

Policy and Procedure Development
A comprehensive, well-thought-out uniform set of written directives, including standard operating procedures and policies will be a critical part of the operation. There are
several issues to be considered as the new Policies and Procedures are developed.

**Personnel Policies:** As part of the policy and procedure development, employment standards and procedures will need to be established. The Executive Committee, in collaboration with the Operations Committee, should develop personnel standards and procedures. There are several issues that will need to be addressed such as:

- Work Week Definition
- Overtime Provisions
- Shift Differential Provisions
- Longevity Pay
- Holidays
- Sick Leave
- Vacation
- Personal/Floating Leave
- Other Leave
- Uniform
- Pay
- Steps and Union Issues (if applicable)

**Training Requirements:** The operational rules and training requirement should be developed and documented in a set of Standard Operating Procedures (SOP). The Operations Committees should develop the SOP.

**Intermutual Agreement (IMA) or Contract:** The IMA or contract is a legally binding document intended to set forth the responsibilities, terms and obligations of the Participating Parties for cost efficient, shared, and effective public safety services.

New partnership opportunities can help agencies make structural changes to address challenging fiscal constraints. While they can take on several forms, any consolidation or partnership should balance funding and governance to ensure positive improvements are made in all aspects of the delivery of public safety services. A well-thought-out IMA, agreement or governance model is essential for your success in these types of collaborations.
For the past decade there has been a great deal of discussion about Next Generation 911 (NG911) as it moved from a vague concept to an increasingly viable reality for public safety emergency communications. The first challenge was to conceptualize the technical requirements associated with the shift from analog to digital and from voice to data. It’s fair to say that much of that work, hard as it has been, is complete and ready to be implemented. The second challenge—one where a lot of work has been done, but where much remains—is to address the operational challenges associated with implementing NG911 in the United States and beyond. In many ways this was almost an afterthought for a while, but clearly progress is being made.

This article will examine the third challenge of addressing the policy implications of NG911, the regulatory and legislative elements of this paradigm shift, and the impact they may have on future technical and operational changes. Taking the initiative early on to think through the issues relative to NG911 implementation—particularly the policy ones—will help ensure success.

From the beginning, there has been a clear understanding that the method(s) of funding NG911 need to be addressed. The traditional surcharge method and other supplemental funding sources would probably not be adequate to address the requirements of building and maintaining a new network, as well as operating a very different type of PSAP receiving data from a variety of sources. The challenges of creating a new funding model, or most likely several different models remain.

However, it is obvious that the work in this policy arena at all levels of government—federal, state, regional, and local—remains essential to ensure the success of NG911 going forward. For the private sector, you must determine how your products and services might fit the particular needs of jurisdictions given their vision of, and progress toward, reaching NG911 functionality. For public sector organizations, challenges include helping create such a vision, implementing the technological and operational functions to achieve it, and proposing a policy framework (legislation and regulations) to ensure its success.

It is important to use the proper approach when pursuing policy changes in a state, county, region, or municipal agency. There are particular policy challenges that might prompt a government agency looking to implement NG911 to seek consulting assistance. For example, it is important to use the proper approach when pursuing policy changes in a state, county, region, or municipal agency. Do policy changes require a legislative approach (either a new statute/by-law/ordinance or amendments to an existing one), a regulatory approach (again either adding regulations or modifying existing ones), or a combination of the two?

It makes sense to implement policy through a regulatory process where there is a history of successful regulatory changes, a clear authority to promulgate such regulations, and some level of understanding of the various NG911 issues by the regulators themselves. In addition, a regulatory process usually has a clear timetable where the legislative process may not.

On the other hand, broader policy issues—particularly funding changes—will almost certainly require legislative approval. This can be a longer and more difficult process, including educating a number of decision makers and stakeholders at both the executive and legislative levels of government. This encompasses elected officials.
(governors, mayors, county commissioners, state legislators, city councilors) as well as key staff in the executive and legislative offices, and organizations that could be affected by these changes.

So the question of regulations vs. legislation may initially focus on legal interpretations of which is best, but it can ultimately end with a political decision as to whether success is best achieved in one particular arena or another. In reality, it is likely to require dealing in both arenas over a period of time—legislation to address larger and broader issues, and regulation to address the more detailed questions. Nevertheless, the politics in a given jurisdiction may be just as important to take note of as the proper legislative or regulatory language needed to achieve a particular goal.

Another aspect of the policy discussion of NG911 is the relationships between and among the different levels of government. Given the requirement for a robust digital network to achieve interoperability across federal, state, county, regional, and municipal lines, it is equally essential that the laws and regulations governing this network, or “network of networks” more properly named, allow for true interoperability to be allowed. This requires a very different policy approach than traditional 911 and its limited analog voice (and limited data) network required.

Much of the early policy thinking, particularly from organizations such as the National Emergency Number Association (NENA), focused on a “jurisdictional policy framework” of how NG911 would operate. There were

The safety of the citizens being served is paramount.
suggested and defined operational, policy, and technical roles for the federal, state, and county/regional/local levels of government. However, this was only a model for discussion and consideration. The real work to implement this intergovernmental relationship continues. What are some examples of what this might look like?

Office of Unified Communications, District of Columbia: The nation’s capital is currently reviewing all aspects of their NG911 program—technical, operational and policy areas. The policy issues are typical for any NG911 implementation, including ensuring the technical and operational needs of the NG911 PSAP are being codified in regulation and statute as needed.

From the policy perspective, questions of funding are paramount, as well as governance to allow the District to run its NG911 system in collaboration with the larger National Capitol Region (NCR). In addition, the District is facing specific policy issues such as establishing legislation on Multi Line Telephone Systems (MLTSs), considering options relative to the management of its ALI database, and seeking to address both long-term funding needs as well as short-term challenges with existing funding sources and revenue streams.

Ultimately the District, as all jurisdictions must do, is developing a comprehensive policy framework to address all aspects of NG911. This framework must include a legislative and regulatory component to ensure that all elements of a successful shift to NG911 are possible.

Commission on State Emergency Communications, State of Texas: As part of a team initiative the State addressed cybersecurity for its NG911 network. Crafting a comprehensive policy, in this case based on guidance from an existing NENA proposed standard, was important to ensure a clear understanding of network governance in a state with various models of providing NG911 services.

Private Sector Technology Providers: Private companies providing services to agencies need to stay abreast of the same policy and regulatory issues to best serve their public safety customers. Private sector interests should seek conversations with key leaders in the states and local government to discuss how mutual success in implementing NG911 can be achieved. In the past, it was thought that state 911 decision-makers should keep a distance from the vendor community to avoid a perception of undue influence from any particular company seeking to gain or retain success. However, it seems increasingly clear that those government leaders overseeing emergency communications agencies must be aware of what is happening with both the existing and new commercial players in the NG911 environment.

As is always the case with emergency communications in general, and 911 in particular, the safety of the citizens being served is paramount. NG911 provides the ability to serve that need in ways that were unimaginable not that long ago to create safer and healthier communities.
Advanced Cyber Threats

PATRICK FLYNN Director, Homeland/National Security Programs, Intel Security

Cybersecurity has become one of the most critical issues facing public safety agencies today and with the development of fully interconnected IP networks such as the Public Safety Broadband Network and NG911, cybersecurity (or cyber defense) will remain at the forefront for the foreseeable future.

Public Safety agencies face the same challenges as our counterparts in the commercial sectors. IT security is an arms race with no commercial breaks, half-time intermission, seventh inning stretch, or finish line. Nonstop innovation by well-organized cybercriminals keeps the frontlines moving and periodically bypasses defensive strategies that once marked the conflict’s cutting edge. Such is the case with signature-based security and today’s advanced malware.

67% of security professionals have no technology deployed specifically to fight advanced malware.

For years, signature-based security alone provided fast, reliable protection from most known attacks, so the more capable hackers inevitably learned to avoid easily identified attacks. Their tactics became stealthy, evasive, defense-aware, and intelligently adaptive. Zero-day attacks and other targeted, advanced malware now frequently challenge the defenses of signature-based intrusion prevention systems (IPS) despite fully up-to-date signature sets. Although signature-based detection provides an important foundation for intrusion inspection, clearly, something more must be done to combat these next-generation malware attacks.

In a survey conducted at the 2013 Black Hat USA conference, 81% of respondents cited advanced malware as a major concern for their organizations, and 35% claimed to spend 10 or more hours each week combatting malware penetrations. In light of those sentiments, it is surprising that 67% of security professionals have no technology deployed specifically to fight advanced malware, according to an Intel Security report published in December 2013.

The New Worst-Case Scenario

This may change as the impacts of the massive malware-enabled data breaches at Target and other retailers sink in. The Target incursion alone appears to have exposed 40 million payment card numbers and compromised the personal data of 70 million customers. The FBI has signaled that further breach revelations can be expected, and investigations are underway at the US Department of Justice, the Secret Service, and in both houses of Congress.

Much remains to be learned about these break-ins, including how the BlackPOS malware made its way onto the retailers’ point-of-sale (POS) systems and how it evaded detection while exfiltrating more than 12 gigabytes of data. But a great deal can be learned about the requirements of advanced malware security by examining a common, well-understood example: a PDF file with malicious embedded JavaScript.

How Signatures Miss Serious Attacks

PDFs have become indispensable tools for platform-independent distribution of rich, interactive content. Email attachments and web downloads carry thousands of PDF files across enterprise firewalls every day, bearing everything from business proposals to software manuals, legal documents, and presentations. To automate various aspects of presentation and interactivity, the format supports dynamic elements, such as dynamic action triggers, remote data retrieval, and embedded scripts.
Scripts have a wide range of useful applications, such as enforcing conditional formatting in a user-populated form so that an email address or phone number can only be entered in the correct format for the designated data type.

What we need is a more sophisticated approach capable of efficiently determining the safety of an unknown executable in the absence of signature-based certainty.

At the same time scripts are an increasingly popular vector for infection, offering an almost-unlimited number of malicious possibilities. A script might download and install a keylogger, rootkit, or bot. Unfortunately, while some IPS can recognize an embedded script, they cannot parse its code or predict its runtime behavior. Unless the IPS scan matches a known threat signature, the file is allowed to pass. When opened on the destination host, the malicious script automatically extracts or downloads a malware payload and installs it on the host. The attack creates new application processes that may capture user credentials and other valuables, export stolen data to a command and control server, or propagate the infection to other endpoints on the network.

Stopping Threats Known and Unknown
How can such attacks be stopped? Signature-based security can only catch attacks that have been previously identified and analyzed, not a new variant making its first appearance. We could simply block all files with embedded scripts, but that would eliminate a popular and useful communication tool. We could send all files with embedded scripts to an offline sandbox for dynamic analysis, but this would delay content delivery and add a large workload to a computationally intensive resource. What we need is a more sophisticated approach capable of efficiently determining the safety of an unknown executable in the absence of signature-based certainty.

To succeed, such an advanced approach must discover new threats through pattern analysis and behavioral prediction, without resorting to historical records of known exploits and incidents. Since no other detection method is likely to match the reliability of a known signature, an advanced approach should apply multiple detection methods in a multilayered stack. It must also limit the false positives generated by intelligently extracting faint threat signals from the normal noise of network activity.

Three Keys: Code Behavior, Traffic Behavior and Reputation
We believe unknown malware attacks can be identified and stopped with high levels of accuracy and reliability by layering three types of analytical techniques over a conventional signature-based defense.

- **Code behavior analysis**: Uses lightweight emulation, sandboxing, and advanced static analysis to assess and predict the behavior of files and executables through direct examination or execution of the code.
- **Traffic behavior analysis**: Identifies malware attacks within the network through behavioral anomalies in the traffic flows they create. These techniques correlate large volumes of network and endpoint events to extract faint threat signals from the background noise of normal network activity.
- **Global reputation analysis**: Adds external context and intelligence to local inspection and assessment.

These detection analytics are applied to unknown threats in a sequence of increasing computational intensity through the appliances that deliver the network intrusion prevention system (IPS).

A signature-less approach, an advanced security offering from several security vendors, can help provide a safer, overall solution. We recommend researching the one that is best for your agency.
The Signature-Less Approach from Intel Security

Let’s examine each of the analytical components that comprise our advanced security offering and the role of each appliance in delivering the overall solution.

**Code behavior analysis:** These signature-less inspection engines leverage emulation and sandboxing technologies to examine files or executables and predict or observe their behavior at runtime (Figure 1). Some are resource-thrifty and operate in near real time; others are more computationally intensive and impose a small increment of latency. Combining them in a sequence of escalating resource intensity provides a cost-effective optimization of performance and effectiveness.

**Real-time deep file inspection:** This is the first line of defense in a multi-tier array of non-signature malware analytics. This feature of a Network Security Platform finds and stops the threats concealed in embedded scripts, as in the PDF example described above. Deep file analysis uses a streamlined JavaScript environment to emulate script execution and predict runtime behavior. Files containing scripts that are observed to be malicious are blocked immediately and at all further appearances. Intelligent script emulation directly on the IPS sensor may be needed. It provides a zero-latency alternative to all-or-nothing script blocking and is far more cost effective than routing all unknown files to a sandbox. In our malicious PDF example, deep file analysis allows a Network Security Platform to identify and block the attack in real time—before the file reaches and infects its target host.

**Real-time emulation:** Real-time emulation is a feature of Advanced Threat Detection that emulates a working...

...clearly, something more must be done to combat these next-generation malware attacks.
environment to study the behavior of entire files (not just the scripts embedded within). Multiple lightweight execution environments are available for a wide range of browsers, file types, and scripting languages, offering a stripped down subset of CPU, memory, and operating system application programming interface (API) resources. These emulators simulate code execution, provide hooks for malicious processes, and predict the resulting behaviors. In addition, heuristic analytics applies rules and pattern analysis to identify similarities between a suspect file and related groups of known threats. Real-time emulation quickly identifies rootkits, zero-day threats, advanced persistent threats, and other advanced malware at a fraction of the computational cost of true dynamic or static code analysis.

**Dynamic code analysis:** The next step when emulation reveals no threats in an unknown file is dynamic code analysis. It is a feature in a Threat Defense appliance, which provides full code execution in a secure virtual machine sandbox. This analysis differs from emulation in that it instantiates a fully operational runtime environment that is isolated to allow safe execution of potentially malicious code. All observed behaviors are logged or classified, including changes to the operating system (OS), files, and registry entries. Unlike sandbox solutions that use a single generic virtual machine (VM) for all analyses (and miss many behaviors that only appear in specific VM configurations), or that test all samples in multiple virtual environments (more thorough but resource-intensive), an Advanced Threat Defense runs each suspicious executable in a virtual environment that exactly matches the system for which the file is targeted. Such software leverages acquired endpoint information and identifies the target host’s specific operating environment, launching a matching VM on the fly. This greatly increases the probability that a file’s full range of potential behaviors are elicited and observed and an accurate assessment is made of its intent. Advanced Threat Defense also emulates appropriate responses to sample behaviors and resource requests (for example, network connections) and offers a fully interactive mode for manual offline analysis.

**Static code analysis:** The indispensable flip side of dynamic analysis. Sandboxing identifies malware with a high degree of confidence based on direct observation of its behavior. It will reliably identify hidden threats in complex executables but can be easily defeated by various strategies. For example, a file may simply outwait the observation period, delaying the start of any revealing behavior for a predetermined interval that may be longer than an economically viable sandbox inspection. Or a file may be programmed to recognize a secure environment by the absence (or presence) of certain resources and execute only a limited set of deceptively innocuous operations.

For these reasons, dynamic analysis should always be paired with true static code analysis. Static inspection provides a window into the nature of latent (non-executing) code for which dynamic analysis is entirely blind. True static analysis identifies structural similarities between latent code and known malware samples, quantifying the percentage of code that executes during a sandbox evaluation, and mapping all of the logical execution paths of a complex file.

**Dynamic analysis should always be paired with true static code analysis.**

On an Advanced Threat Defense appliance, true static code analysis launches concurrently with dynamic analysis and incorporates some of its outputs when available. Unlike many available static malware analysis technologies, this inspection fully unpacks and reverse-engineers obfuscated code to recover intact versions of disassembly code. These are then parsed and subjected to statistical analysis, providing:

- An assessment of similarity with known malware families
- A measurement of the latent code that did not execute during dynamic analysis
- A logical map of the file’s complete execution path(s)
These findings are then incorporated with the observations from dynamic analysis to provide an overall threat score indicating the degree of certainty that the sample file or executable is malicious.

**Traffic behavior analysis:** These signature-less inspection methods look at behavioral patterns in traffic flows to find anomalous signals hidden in the background noise of normal activity, no matter how faint.

**Endpoint Intelligence Agent:** This agent provides real-time, per-flow endpoint traffic correlation by positively associating every network session with the originating host system, user, and application process. This solution leverages intelligence in the network and on every Microsoft Windows host to reveal relationships between endpoint executables and network traffic flows, making it possible to:

- Identify malicious network connections and executables in near real time
- See detailed process context for every attack
- Block malicious communications and prevent the spread of advanced malware
- Quarantine and remediate compromised host systems

The Endpoint Intelligence Agent acquires its host system insight from a small-footprint, plug-and-play software module deployed from the endpoint system. When installed and configured, the agent inventories all application processes on the host and monitors their communication activities. Each time a process requests a network connection, the agent first sends a tiny packet of metadata to network security services. This packet includes information about the connection (message protocol, source, and destination address and port), the user (name and security identifiers—but no secure personal information), and the endpoint application process (application name and hash). Security services in the network combine this endpoint and session data with reputation intelligence on the source and destination endpoints, allowing a high-confidence threat assessment of the pending communication and the internal endpoint’s security state. Communication attempts by compromised hosts can then be quarantined so that malicious traffic within your network can be controlled. By quarantining the infected host and blacklisting the identified malware, exfiltration of valuable data is prevented and impact on the network is limited.

No potential security partner offers as complete a portfolio of advanced, post-signature detection technologies or combines them as effectively with traditional signature-based security as we do.

**Advanced botnet detection:** This is a layer of traffic and network event correlation specifically dedicated to botnet security, one that far exceeds the signature-based identification and detection algorithms of the past. A Network Security Platform correlates multiple individual network alerts or anomalies and applies heuristics to reveal the true fingerprints of botnet infections. This multi-activity correlation provides threat identification with a far higher degree of confidence than individual, single-activity signatures can provide.

For instance, advanced botnet analysis might correlate an apparently unrelated DNS website query with a PDF download and a sudden traffic surge between an internal endpoint and a high-risk web domain. Individually, none of these events might be sufficient to convict the internal endpoint, but, considered in aggregate, the evidence could justify action to isolate, investigate, and remediate. Advanced botnet protection sequences, correlates, and weighs a wide range of events and activities to pinpoint bot infestations that are invisible to other defenses.

**Network threat behavior analysis:** Network Threat Behavior Analysis is an in-network correlation engine that applies behavior-based algorithms to network traffic data. It brings together netflow data from switches, routers, and other network devices from Cisco, Juniper,
and Extreme Networks, combining them with layer-7 application traffic data from the Network Security Platform and reputation intelligence. From these sources, it automatically creates models of normal bandwidth consumption, by each application, of host-to-host traffic volume and encryption utilization and then applies the models to identify and bring forward the subtle anomalies that reveal successful penetrations.

Network Threat Behavior Analysis drills down into complex, multivector attacks and blended threats. It holistically evaluates network-level threats, identifies the overall behavior of each network element, and instantly abstracts apparent anomalies to identify distributed denial of service (DDoS) attacks, zero-day threats, botnets, worms, and reconnaissance attacks—in real time and entirely without signatures.

**Post-Signature Malware Security Solution**

The malware threat landscape is always changing, and network security practices evolve on its heels. Signature-based defenses remain essential as the most efficient way to stop the millions of known attacks, but signatures alone cannot stop today’s advanced, evasive malware. Effective security now requires signature-less malware detection that leverages multiple detection strategies and deployed in multiple overlapping tiers. No potential security partner offers as complete a portfolio of advanced, post-signature detection technologies or combines them as effectively with traditional signature-based security as we do.
Current and future challenges related to crafting, updating, and maintaining public safety communications systems are multifaceted, with crucial factors both known and unknown. The ability to analyze the known, and ferret out the unknown, is dependent upon having a robust team of skilled professionals on hand to address the many complex issues that unfailingly arise, and to aid in paving a path to successful solutions.

By issuing this Guide, the contributing authors – along with the full range of iCERT’s membership – aim to promote a climate of early-stage and ongoing collaboration between public and private entities, as both seek to ensure effective deployment of emergency services. From the initial stages of developing Requests for Proposals, through the procurement and internal governance processes, as well as the inclusion of network protections, and on to efforts needed to ensure long term financial support for critical services, private sector experts – iCERT’s member companies – stand ready to engage with public safety experts toward the mutual goal of delivering life-saving services to the public.

The insights shared throughout the sections of this Guide are infused with knowledge gleaned from years of experience, and brought to the reader from a place of understanding and accomplishment, through working within and alongside public agencies. They represent a unique look into the workings of public-private partnerships, and serve as a testament to iCERT members’ commitment to public safety.

Best Regards,

George Rice
Executive Director
geroge.rice@theindustrycouncil.org
+001 240-398-3065
About the Authors

**David F. Jones**, ENP | Principal and Senior Vice President, Mission Critical Partners

Jones provides executive-level consultative services and expertise on matters related to Next Generation 911, government affairs, public policy, and legislation. He is an internationally known subject matter expert on 911, Next Generation 911 (NG911), and emergency services. He has advocated for emergency services-related issues throughout North America, as well as in India, Brazil and Iceland.

He was among the first in the nation to be certified as an Emergency Number Professional (ENP) and has more than 30 years of experience in the public sector, where he administered, directed, managed, and operated emergency service agencies and 911 departments.

**Cheryl S. Giggetts**, MBA, CHS III | Senior Vice President, AECOM

Giggetts is a Senior Vice President at AECOM directing Technology Solutions, a global provider of wireless services. She has more than 30 years of experience in management, and 27 years in the Wireless Telecommunications industry, highly specialized in Public Safety Communications and E911 Services for local, state, and the federal government.

Her responsibilities encompass global strategic management, technology integration, and cross-functional team development. Her experience also includes developing strategies for funding, sustainability and governance. An integral part of developing these elements involves gap analysis, risk analysis, and risk mitigation, which provide the foundation for a successful project/program.

**Paul Fahey**, Senior Consultant, Winbourne Consulting

Paul Fahey is a Senior Consultant for NG911 Projects and Programs with Winbourne Consulting. He has 15 years of experience in emergency communications, including service as Executive Director of the Massachusetts State 911 Department, Executive Director of the 911 Industry Alliance, and Director of Association and Government Affairs for Cassidian Communications.

He is also a former Board member of the Industry Council for Emergency Response Technologies, the E911 Institute, the National Association of State 911 Administrators, and the Denise Amber Lee Foundation.

**Patrick Flynn**, Director, Homeland/Security Programs, Intel Security

Patrick Flynn is a public sector security expert with more than 25 years of experience in the federal government, in addition to his experience serving governments’ needs in the private sector. He is the Director of Homeland/National Security Programs for Intel Security (formerly McAfee), previously serving in similar roles at Northrop Grumman and General Dynamics.

Flynn’s public sector experience includes work at the U.S. Department of Homeland Security as the Director of Communications of the Joint Wireless Program Office. He serves on the President’s National Security Telecommunications Advisory Council, most recently co-chairing the production of the Information and Communications Technology Management Service Mobilization Report.
Additional Resources

History of 911: A Policy and Technology Reference Guide
This report is designed to educate public and private sector stakeholders about the importance of 911’s history as it relates to its technical and policy origins, its current status, and its future development into NG911.

iCERT NG911 Research Report - April 2015
iCERT report on America’s readiness for transition to NextGen 911 technologies, with applicable insights for adoption of IP-based three-digit emergency calling around the globe.

The Overloaded 911 System
This report highlights examples of overload to the U.S. 911 system for a variety of reasons.