The National 911 Program

Next Generation 911 Procurement Guidance

Washington, DC
October 2016

911.gov

Table of Contents

Executive Summary

Public safety answering points (PSAP) require a unique understanding of the specialized technology that provides the conduit between the public and law enforcement, the fire service and emergency medical services (EMS). PSAPs are filled with complex and interrelated systems such as 911 call handling equipment (CHE, formerly known as customer premises equipment, or CPE), computer-aided dispatch (CAD) systems, records management systems (RMS), geographic information systems (GIS)/mapping interfaces, administrative phone systems, digital logging recorders, ergonomic console furniture stations, radio console equipment, radio system equipment, and redundant data/voice radio circuits and systems.

Planning for the initial purchase, replacement or upgrade of such equipment requires specific knowledge of the equipment but also requires an understanding of the procurement process, knowledge of contracts and the ability to negotiate them. Ensuring that contractors can be held accountable for delivering the required equipment and services once a contract is awarded requires an understanding of what specific steps need to occur as part of the procurement process, and a working knowledge of the essential role of contract language. The importance of establishing contract terms and conditions "up front" cannot be overestimated. Yet, most PSAP Managers and 911 Authorities do not receive education or training on contract language or the procurement process used by their level of government (federal, local or state). The purpose of this document is to provide information to begin bridging that gap.

This document contains three sections. The first two provide background and discuss the application of this information, while the third section focuses on three areas of consideration regarding contract negotiation and documentation:

- **General Contract Considerations:** provides information to ensure that the contract meets general Terms and Conditions (T&Cs), that standard contract terms are addressed, and that the jurisdiction's needs and requirements are clearly understood and the jurisdiction is protected from vague references and unclarified specifications.
- **Service Level Agreements (SLAs):** defines what should be spelled out in a contract to ensure that the jurisdiction has a successful project and receives the deliverables it requires
- **Security:** provides information to ensure 911 systems are resilient to cyber-attacks and data will be secure from breaches, Trojan horse, viruses, phishing, redirections and unauthorized access.

As with any 911-related contract, there are many moving parts and participants. However, the one "customer" in this process that cannot be expected to be flexible is the public. The primary goal of this entire effort is to procure and implement Next Generation 911 (NG911) equipment and services in a seamless manner, in order to provide reliable, uninterrupted service to the public.

1. Background

Today's 911 emergency communications professionals face challenges on multiple fronts—a fundamental lack of resources, aging equipment operating past its intended lifecycle, emerging consumer technology that has outpaced PSAP upgrades, and outdated funding models that do not consider the dwindling number of landline subscribers and the continued increase in the number of consumers choosing wireless and alternate telephony providers.

There is a clear need to upgrade to NG911. One of the first questions to answer is: "What exactly is NG911?" There are multiple definitions from reputable sources about what constitutes NG911. The National Emergency Number Association (NENA) glossary definition describes NG911 as:

> *. . . an Internet Protocol (IP)[1] based system comprised of managed Emergency Services IP-based networks (ESInets), functional elements (applications), and databases that replicate traditional E9-1-1 features and functions and provide new capabilities. NG9-1-1 is designed to provide access to emergency services from all sources, and to provide multimedia data capabilities for PSAPs and other emergency service organizations.*[1]

In 2009, the U.S. Department of Transportation (USDOT) created a Next Generation 911 (NG911) Procurement Tool Kit[2] as part of their NG911 Initiative. The Tool Kit describes the essential steps in planning for NG911, and outlines the resources available to assist 911 authorities in their efforts to help improve communications among the various individuals, groups, and companies interested in NG911.

The Procurement Tool Kit has four parts, and contains tools to assist with assessment, planning, procurement, and evaluation. The procurement tool offers guidance for procuring goods and services associated with a transition to NG911. Because not all organizations have the same experience and/or skills in purchasing information technology (IT) solutions, the tool includes a "best value" process that may help improve individual procurement efforts.

The National 911 Program (the Program), housed within the Office of Emergency Medical Services (EMS) at the USDOT's National Highway Traffic Safety Administration (NHTSA), has developed this NG911 Procurement Guidance document to provide a resource for 911 entities during the next step of the procurement process. This document is intended to provide assistance to 911 authorities as they negotiate contracts and scope of work (SOW) documents for network enhancements and NG911 services after the initial procurement process is complete.

Based upon information learned from previous procurements within the 911 community, there is a basic set of considerations that a 911 Authority or PSAP Manager might want to include in a procurement document, or review as part of the contract negotiation phase of procurement.

[1] National Emergency Number Association, Glossary: http://www.nena.org/glossary
[2] Available at: http://www.its.dot.gov/ng911/pdf/USDOT_NG911_Procurement_ToolKit_2009.pdf

2. Using This Document

When a 911 authority is looking to procure NG911 goods and services, this document can be used to ensure that the procurement document is complete and effective. In addition, this document can provide a checklist of items to consider during the contract and SOW negotiation phase. This document is not intended to provide comprehensive, detailed instructions on how to create a procurement document or negotiate contracts; rather, it offers a high-level list of considerations.

All of the items in this document may not be applicable for all agencies, depending on whether the jurisdiction is a federal, state or local PSAP or supporting agency. Each 911 entity is governed by local or state procurement requirements that may affect how the suggested considerations are employed.

3. Procurement Considerations

The procurement considerations in this document are organized into three distinction sections:

- **General Contract Considerations:** provides information to ensure that the contract meets general Terms and Conditions (T&Cs), standard contract terms are addressed, and the jurisdiction is protected
- **Service Level Agreements (SLAs):** defines what should be spelled out in a contract to ensure that the jurisdiction has a successful project and receives the deliverables it requires
- **Security:** provides information to ensure 911 systems are resilient to cyber-attacks and data will be secure

3.1. General Contract Considerations

General contract considerations are often required by the local procurement authority, and a standard set of T&Cs are typically included as part of the procurement process or incorporated in the resulting contract. This section highlights additional considerations that may not be automatically addressed by standard procurement processes.

3.1.1. General Terms and Conditions (T & C)

There are some general T&Cs (that will vary by both language and applicability based on procurement requirements for each jurisdiction) that are contractually considered non-negotiable. Below is a list of T&Cs that may be included as non-negotiable items in a contract:

- An indemnification clause which is a contractual obligation by one party, [X] to pay or compensate for the losses or damages or liabilities incurred by another party [Y] to the contract or by some third person.
- A Force Majeure clause is a contract provision that relieves the parties from performing their contractual obligations when certain circumstances beyond their control arise such as natural disasters like hurricanes, floods, earthquakes, and weather disturbances sometimes referred to as “acts of God.”
- Pricing – jurisdictions may have a specific method for pricing

- Responsibility of equipment – for example, the jurisdiction assumes no responsibility for equipment left on its property
- Ownership – for example, the vendor maintains ownership of the equipment until PSAP final acceptance
- Historically Underutilized Businesses (HUB)
- Minority and Women-Owned Business Enterprises (M/WBE)
- Compliance with all applicable laws – federal, state and local
- Insurance requirements
- Drug-free workplace
- Taxes
- Court jurisdiction
- Request for proposals (RFP) preparation cost – the vendor typically is responsible for the cost of responding to the RFP
- Late proposals – they typically are not considered
- Contract duration
- Non-Disclosure Agreement (NDA)

3.1.2. Project Management Structure

Each project will be unique and should be managed as such. The contracting jurisdiction should assign a project manager/program manager (PM) to act as the primary point of contact and work alongside the vendor's PM. This individual should have intimate knowledge of the project, contract requirements, project goals, and the intended outcome. The PM's role is to ensure that the vendor is meeting all of the contractual agreements pertaining to the project, including deliverables, timelines and testing, and all administrative contractual obligations.

The contracting jurisdiction may want to impose certain requirements for a vendor's PM. These requirements may include, depending on the project, a requirement for years of experience as a measure of expertise, experience working on similar projects of size and scope, a certain technical degree, and/or a Project Management Professional (PMP) certification. The vendor should provide the percent of time the PM will dedicate to the jurisdiction's project; this also applies to all other individuals assigned to the project. It is also important that the contracting jurisdiction retains the right to replace the PM or any service provider whose performance is deemed below par or is detrimental to the success of the project. This is often referred to as the designation of "key personnel" and establishing the contracting jurisdiction's requirement for "approving" the person assigned to the PM role.

Some contracting jurisdictions may require that the contract delineate specific terms for what the vendor and its PM are expected to provide and accomplish, and how this will transpire. Items for consideration include the following:

- Project management methodology should be mutually agreed upon
- The tools the vendor's PM uses should be mutually agreed upon

- The contracting jurisdiction may want the PM to maintain an "Action Item Register" to track progress
- The contracting jurisdiction may want the project timeline updated weekly to closely follow progress
- The contracting jurisdiction may want meeting notes completed in a specific timeframe after a meeting
- The meeting schedule should be determined by the customer, not the PM
- Version control of the documents is a must and should be managed by the vendor's PM
- Change management should be defined by the customer; some jurisdictions have a standard method of managing change

Reporting and Metrics

The contracting jurisdiction should request regular progress reports that contain, at a minimum:

- A summary of accomplishments,
- Adherence to timelines/milestones and adjustments,
- Punch list items, action items, outstanding issues, and progress reports,
- Any noteworthy activities, events, or successes,
- Any issues that introduce risk for project success or completion and mitigation strategies,
- A Financial Statement of funds expended to date as well as percentage of funds expended compared with percentage of tasks or timeline,
- Installation progress at the site or sites,
- Testing and acceptance as agreed upon by the jurisdiction, and
- Other metrics, which should be tied to system performance, such as outages, uptime or other quantitative measurements. Damages can and should be assessed when there is failure to meet these metrics, and the specific nature of these damages should be established in the contract.

Real-Time Dashboards

Some vendors may include a methodology for communicating the progress of the project through a dashboard that provides real-time data, such as project plans, timelines, milestone schedules, task and action items; the dashboard also should produce standard reports and a method of collaborating with team members.

3.1.3. Escalation Procedures

Escalation procedures are usually included in services-based contract to identify particular thresholds that, when exceeded, specify the process to follow for additional levels of attention or response for an issue. It is important to determine and document the order of precedence regarding escalation procedures for addressing any contractual disagreements that may arise. Most procurements involving purchases of significant equipment or services begin with an RFP and/or a request for qualifications (RFQ) from the contracting jurisdiction to all potential bidders. Responding vendors will submit a proposal. After the proposals are reviewed and evaluated, the contracting jurisdiction and selected vendor will enter into a contract for equipment and/or services. It is important to have the vendor's RFP

response incorporated into the contract, and it should be determined whether the contract or RFP response takes precedence in the event a dispute arises.

During the contract negotiations, it is important to identify the order of precedence of the contract documents and to determine, before the negotiations start, which issues are negotiable and which are non-negotiable. Typically, the contract takes precedence; however, there are exceptions and sometimes the RFP and/or RFQ are referenced and incorporated into the contract, along with other information such as addenda, amendments, vendor's proposal, electronic recordings of the presentation, and the presentation materials. Also, the customer, the contracting jurisdiction in this case, should try to establish that any court jurisdiction for legal dispute be adjudicated in their state.

There are various ways to handle a dispute; one method is to form a Dispute Resolution Panel. In the event a dispute concerning the contract arises between the jurisdiction and vendor, and it cannot be resolved between the parties, the dispute could be escalated to the Panel. Each party to the contract shall appoint one member to the Panel. These two appointed members shall jointly appoint an additional member. The Panel shall review the facts, contract terms and applicable statutes and rules, and then make a determination on the dispute as quickly as reasonably possible. Local customs or regulation may already provide for this situation and should be followed.

Another method involves Third-Party Arbitration. This is a technique for the resolution of disputes outside the courts. The parties to a dispute agree to be bound by the arbitration decision by a neutral third party. The third party reviews the evidence in the case and imposes a decision that is legally binding on both sides and enforceable in the courts. Another option involves Mediation, which is generally conducted with a single mediator who does not judge the case but simply helps to facilitate discussion and eventual resolution of the dispute. Unlike arbitration, mediation is not enforceable by the court and if not successful could lead to litigation. Local custom or regulation may already dictate the use of escalation procedures for disputes. The contracting jurisdiction is advised to consult with the agency responsible for procurements as well as their legal department, to understand the escalation procedures utilized by the agency, and any specific actions that are required as part of the escalation procedure.

3.1.4. Standards Commitments

Standards affect the daily lives of everyone across the nation. From the most mundane aspects of life (e.g., electrical cords and wall sockets) to potentially life-and-death situations (e.g., the concentration of ingredients in generic medications), standards guide the quality, safety, and security of products or processes. Standards are widely used in all areas throughout the U.S. government and public and private sectors. Because of the very definition of NG911, i.e., "a network of networks," standards are required to ensure that one system can interact with other systems in order to provide a nationwide seamless network.

When procuring NG911 equipment and services, it is essential that the vendor adhere to national standards in order to ensure interoperability. The standards required should be listed within both the RFP document and the contract.

Interoperability requirements represent another important consideration for PSAPs. Such requirements will vary from site to site. The jurisdiction will want to ensure that the equipment it is purchasing works seamlessly with current equipment and systems. For instance, if purchasing a new CAD system, ensure that it will interface with the current RMS and other equipment. Always ensure that all interfaces are listed in the RFP, as well as in the contract. The contracting jurisdiction may also want to confer with surrounding jurisdictions, to understand the specifics of their equipment and services, as part of a comprehensive plan to ensure seamless interoperability.

Public Safety Grade

When negotiating for any public safety equipment, whether it be a building, hardware, software or other item(s), there is usually a specific grade or standard that is required or recommended to meet public safety requirements. "Public Safety Grade" is a conceptual term that refers to the expectation of the 911 industry and more broadly, emergency response providers and practitioners, that their equipment and systems have been designed with security, reliability, resiliency, redundancy, and diversity in mind. Further, these systems and networks will remain fully operational during regular daily operations as well as during and immediately following a major natural or manmade disaster on a local, regional, and even nationwide basis.

NENA has established numerous standards for, and has published white papers on, various types of equipment[3] and requirements for applications and services. Similarly, the National Fire Protection Association (NFPA) 1221 standard[4] recommends best practices regarding public safety structures and equipment. There also are grounding standards, such as Motorola R56®. Finally, it is imperative that GIS data is public safety grade, as it will be used in a NG911 environment to locate emergency callers. Potential contractors should be required to include in their proposals, specific information on exactly how they would meet or exceed any standards included in the specifications for equipment or system performance.

3.1.5. Upgrades/Maintenance Procedures

Upgrades and version management should be addressed in the contract to ensure that the equipment and/or software remains current. The implementation of upgrades, regardless of kind (e.g., hardware, software, security patches, configurations, etc.) should have no impact on 911 call processing or operations during the upgrading process. Upgrades and maintenance should be scheduled with the jurisdiction in advance to ensure that these occur during off-peak times and/or weekdays. All of these upgrade and maintenance procedures should be specifically included in the contract document to ensure the contractor can be held accountable for these activities.

3.1.6. Fees and Billing Triggers

Typically, there are two types of pricing models: Firm Fixed Price and Time and Materials (T&M). Firm Fixed pricing is exactly as it sounds—a contract establishes a price that is not subject to any adjustment

[3] NENA Standards Page: http://www.nena.org/standards
[4] NFPA 1221: *Standard for the Installation, Maintenance, and Use of Emergency Services Communications Systems*. Available at: http://www.nfpa.org/codes-and-standards/document-information-pages?mode=code&code=1221

on the basis of the vendor's cost while executing the contract and completing the project. This contract type places maximum risk and full responsibility for all costs of the project on the vendor. In contrast, a T&M project is one where the jurisdiction agrees to pay the vendor based upon the time spent by the vendor's employees and/or subcontractors to perform the work, and the cost for any materials and/or travel needed to complete the project. With a T&M contract, it is often necessary for the vendor to provide additional data explaining the work performed with the billing.

Billing triggers should be tied to milestones such as customer-approved deliverables and/or acceptance, as opposed to billing dates, as dates may come and go without milestones being met. Ensure that deliverables and acceptance are defined clearly in the contract and/or RFP. Communications protocol is very important and it is critical that the vendor notify the PM when specific items, such as hardware (items that take up space), are being delivered. When defining deliverables and product acceptance, the more specific the better. It may be in the best interest of the contracting authority to try, as much as reasonable, to tie a meaningful percentage of the total project cost to acceptance, particularly concerning software or integration services. Hardware delivery and installation is a deliverable and should be paid as such.

Acceptance of any equipment or software should be clearly defined in the RFP and/or the contract, and the warranty period should not start until final acceptance testing is successful and complete. The acceptance criteria, for example, could be 30 days with “five nines,” i.e., 99.999 percent uptime. If the acceptance testing fails at any point, the acceptance test period should restart. Also, if purchasing for a region or state, ensure that the acceptance is for each PSAP or piece of equipment, and not an average of all.

Billing Disputes

Detailed invoices must be required and reviewed upon receipt. Billing requirements and billing disputes should be detailed in the contract so that both parties understand the billing schedules, what is to be billed, specific invoice requirements, and how discrepancies will be addressed. Dispute resolution was discussed in Section 3.1.3 Escalation Procedures above, and is applicable to billing disputes as well.

3.1.7. Financial Security

As part of the contract, the selected vendor should provide financial data that proves it is financially stable and able to perform the project as contracted. Review of third-party information sources, such as Dun & Bradstreet (D&B), may provide independent verification of a vendor’s financial security.

3.1.8. Bid Bonds and Performance Bonds

A bid bond is issued as part of a bidding process by the vendor to the jurisdiction, in order to guarantee that the selected vendor will undertake the contract under the terms at which it bid. The bond amount is subject to full or partial forfeiture if the selected vendor fails to either execute the contract or provide the required performance. In general, bid bonds are used to establish and confirm that the selected vendor is qualified to undertake the project.

A performance bond is a surety bond issued to guarantee satisfactory completion of a project by a vendor. (A project requiring a performance bond usually will require a bid bond as well.) For example, if the vendor fails to deliver the product according to the terms of the contract, the jurisdiction is guaranteed compensation for any monetary loss up to the amount of the performance bond.

3.1.9. Data

The jurisdiction should ensure the contract stipulates ownership of all rights and title to its data that is used in relation to any product or service being procured. Vendors should describe how their proposed solution stores and retrieves information for reporting purposes, including portal access and ad hoc reporting features. The description should include comments regarding any requirements made upon the jurisdiction for this feature. The contracting jurisdiction should never assume full access to data, and should specifically include language related to their access to and use of data as part of the contract document.

Protection of data should be an integral part of the business activities of the vendor to ensure there is no inappropriate or unauthorized use of the jurisdiction's information at any time. The vendor should safeguard the confidentiality and integrity of the jurisdiction's information. General security requirements are discussed in more detail in Section 3.3, below.

Location of the stored data and availability of the data are important aspects of the contract, particularly for a cloud environment. Data stored in data centers outside the United States are subject to the laws of that country. Therefore, it is important for public safety agencies to ensure their data is being stored in the United States.

3.2. Service Level Agreements/Network Operations Center and Help Desk Procedures

A service level agreement (SLA) is a contract between a service provider/vendor and the jurisdiction that defines the level of service expected from the service provider/vendor, how the vendor will meet that level of service, and the penalty for non-compliance. SLAs are output-based in that their purpose is specifically to define what services the jurisdiction will receive.

3.2.1. Network Operations Center (NOC)/Help Desk Procedures

The level of warranty, maintenance, and service should be defined in the contract. Whether it be on-call or 24 x 7 monitoring, vendors should have processes and procedures for supporting a NOC that can rapidly triage calls. However, a NOC for public safety equipment and operations should be staffed to support 24 x 7 restoral or mitigation of incidents, and should provide a 24 x 7 toll-free number. This level of service is sometimes a cost consideration. As mentioned, some vendors will offer to monitor the system on a 24 x 7 basis, but this does come with a cost. In any warranty or maintenance agreement, ensure that all hardware, software, cabling and connectors are covered.

3.2.2. Performance

Performance measure include response time and outage reporting. Response time is more than a vendor acknowledging a problem exists, but providing a repair, problem resolution, or restoration of service. Depending on the severity and type of issue, some contracts may require a repair technician or representative to be physically present at the customer's facility within a specified timeframe.

Response Times

Response times should be based on the severity of the incident, which is defined by the type of problem. For example, a Severity Level 1 incident could be defined as a complete system failure requiring an accelerated response time; a Severity Level 2 incident may require twice the response time of a Severity Level 1 incident. Meanwhile, Severity Level 3 and Severity Level 4 incidents, as well as routine maintenance, could have a response time of several days. The contract language also should specify damages should the vendor be unable to provide the agreed-upon services.

Below is an example for defining severity levels for responding to and reporting on network and/or system outages or failures:

- Severity Level 1 and Severity Level 2 incidents responded to within X minutes
- Severity Level 1 incidents resolved within X hours
- Severity Level 2 incidents resolved within 2 x X hours
- Severity Level 3 incidents resolved within 10 x X hours
- Severity Level 4 incidents resolved within 20 x X hours

Within the Information Technology Service Management (ITSM) framework, common definitions of the severity levels identified above are as follows:

Severity Level 1 Incident

An incident shall be categorized as a "Severity Level 1 Incident" if the incident is characterized by the following attributes: the incident (a) renders a business critical system, service, software, equipment or network component unavailable or substantially unavailable, or seriously impacts normal business operations, in each case prohibiting the execution of productive work, and (b) affects either (i) a group or groups of people, or (ii) a single individual performing a critical business function.

Severity 2 Incident

An incident shall be categorized as a "Severity 2 Incident" if the incident is characterized by the following attributes: the incident (a) does not render a business critical system, service, software, equipment or network component unavailable or substantially unavailable, but a function or functions are not available, substantially available, or functioning as they should, in each case prohibiting the execution of productive work, and (b) affects either (i) a group or groups of people, or (ii) a single individual performing a critical business function.

Severity 3 Incident

An incident shall be categorized as a "Severity 3 Incident" if the incident is characterized by the following attributes: the incident causes a group or individual to experience an incident with accessing or using a system, service, software, equipment or network component or a key feature thereof and a reasonable workaround is not available, but does not prohibit the execution of productive work.

Severity 4 Incident

An incident shall be categorized as a "Severity 4 Incident" if the incident is characterized by the following attributes: the incident may require an extended resolution time, but does not prohibit the execution of productive work and a reasonable workaround is available.

Outage Reporting

For major outages, the vendor shall provide the jurisdiction with a Reason for Outage (RFO) report within an agreed-upon timeframe. For minor outages, this timeframe may be on a weekly basis or as agreed upon. The jurisdiction should expect a timely resolution plan with the RFO report.

3.2.3. Event and Incident Management

As products are installed, tested and accepted, events and incidents will occur along the way. Ensure the vendor manages such events and incidents by logging, numbering, and tracking them. Request weekly or monthly updates on events and/or incidents, or ask for the ability to view the vendor's tracking system in real time. In addition, it is reasonable to ask to view other customers' event and incident logs. Vendors may resist providing this information, but such information can provide insight into issues of which the jurisdiction should be aware.

3.2.4. Network Quality Metrics (e.g., jitter, latency, mean opinion score [MOS])

The jurisdiction should require each vendor to provide quality metrics for its proposed network when responding to the RFP. Once a vendor is selected, the contract SLAs should require that the vendor meet the metrics provided in its RFP response. The SLAs also should specify that the metrics must be met over a specific period of time or a penalty will be assessed.

3.2.5. Network Redundancy and Resiliency

The RFP should require that the vendor has a physically diverse redundant path. It is suggested that an open-ended question be included in the RFP to verify the vendor understands the difference between redundancy and resiliency. The SLA should define the resiliency and redundancy requirements, with penalties assessed for nonconformance.

3.2.6. Availability

The availability requirements for the NG911 network and related components should be defined within the RFP, and it is suggested that the vendor identify the amount of time needed for an element switch. The vendor's response to that question will allow the jurisdiction to determine if the vendor will meet the availability requirements. The SLAs should document the requirements and reference the severity levels, in order to detail the process for resolving any failure, along with penalties for nonconformance.

3.2.7. No Single Point of Failure

Mission critical systems must be designed and implemented with no single point of failure. Redundant equipment with appropriate backup or failover solutions must be provided.

3.3.Security[5]

"It is the policy of the United States to enhance the security and resilience of the nation's critical infrastructure and to maintain a cyber environment that promotes safety, security, business confidentiality, privacy, and civil liberties."[6] As local 911 systems begin to transition to next-generation, IP-based network infrastructures, it is critical that the systems are resilient to cyber-attacks, and citizens know their data will be secure. By collaboratively implementing risk-based security standards on next-generation networks, we can ensure that 911 systems stay secure and that citizens' private information stays safe while traveling over 911 networks. Specific cybersecurity language should be included in any contracts for 911 related equipment or service, and the following section contains ideas for inclusion as part of contractual language.

3.3.1. Security Network Critical Functions

The National Institute of Standards and Technology (NIST) Cybersecurity Framework states that secure networks rely on five critical functions: Identify, Protect, Detect, Respond, and Recover.[7] These functions provide a high-level understanding of a network's security risks and will allow 911 authorities to accurately assess their networks over time. The categories are described as follows:

- **Identify** – Develop organizational understanding to manage cybersecurity risk to systems, data and capabilities.
  - Anytime the system is upgraded, the 911 authority should ensure that the vendor is required to reassess permissions and security settings on the system before delivery. (Assessment)
  - The vendor should be required to disclose its Information Security Plan, and update and revise it as necessary. (Assessment)
  - The vendor and 911 authority must work together to ensure the security, integrity, and confidentiality of non-public information. (Governance)
    - Explanation: At the very least, vendors must be required to ensure that the 911 entity's non-public information is protected and confidential while traveling over their networks. Compliance with local, state, or federal privacy laws must be assured.
  - Vendor should be required to disclose all known risks to private data to operators. (Risk management strategy)
    - Explanation: This requirement ensures that 911 authorities are aware of the risks associated with collecting information over their next-generation networks or systems.

[5] The section on cybersecurity for next generation 911 networks was contributed by University of Colorado Law Students Allison Daley and R. Kolton Ray

[6] Executive Order 13636, February 12, 2013. https://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity

[7] Available at: http://www.nist.gov/cyberframework/

Under certain conditions, PSAPs may be required to disclose the possibility of a breach to citizens before they can collect any personally identifiable information. By requiring transparency, 911 authorities will have more knowledge relating to possible breaches and can provide their customers more-informed assistance.

- Vendor should be required to be available to answer cybersecurity-related inquiries by operators and disclose the best people for the contracting jurisdiction to contact with questions. (Asset management/business environment)
  - Explanation: This requirement ensures that the vendor will be willing and available to answer cybersecurity-related inquiries by 911 authorities using their network. This is an important clause because it ensures that PSAP operators and 911 authorities are able to ask questions when necessary, which will provide added security to the network overall.

- **Protect** – Develop and implement the appropriate safeguards to ensure delivery of critical infrastructure services.
  - The 911 authority must ensure that the vendor contracts to protect against any anticipated threats or hazards to the security or integrity of non-public information. (Data security)
    - Explanation: This clause places the burden of responsibility in fixing any issues regarding the security, integrity or confidentiality of private information on the vendors themselves. When vulnerabilities arise, it is vital to the security of networks for the network operator to investigate and patch the system to protect non-public information.
  - The vendor should be required to review and disclose its Information Security Plan on occasions that should be specified in the contract. (Maintenance/protective technology)
    - Explanation: Threats to network security are constantly evolving, and it is vital to network security for vendors to review their information security plans on a regular basis.[8] [9] Vulnerabilities and system bugs are found each and every day, and what has worked in cybersecurity yesterday may not be the best practice today. In order to keep up with changing trends in cybersecurity, it is absolutely vital that the vendor review its Information Security Plan, or equivalent, at least once a year to evaluate any new vulnerabilities that could lead to a data breach.
  - Anytime the system is upgraded, the 911 authority should ensure that the vendor is required to reassess permissions and security settings on its baseline system before delivery. (Access Control)
  - The 911 authority should ensure that the vendor commits to protecting against unauthorized access to, or use of, such information that could result in harm or inconvenience to the person that is the subject of non-public information. (Data security), and provides details on specifically how this task will be accomplished.

[8] TechRepublic: *10 Common Network Security Design Flaws*, *at* 1. Available at: http://www.techrepublic.com/blog/10-things/10-common-network-security-design-flaws/

[9] NSA's *Manageable Network Plan* at 30. Available at: https://www.iad.gov/iad/library/ia-guidance/security-configuration/networks/manageable-network-plan.cfm

        - Explanation: It is critical to the security of networks that user permissions are managed correctly.[10] The weakest point of any network is the user, so ensuring that access is restricted to only those who require access is necessary for system security.[11] Additionally, both general and user-specific network security settings must be monitored to ensure that there are no vulnerabilities that can be easily patched. These risks increase when a network is updated due to oversight and error, thus vendors should reassess permissions and security settings on their baseline systems before upgrades are implemented.
    - The 911 authority should reduce risks associated with any supplier having access to information resources. (Access Control)
    - Both the 911 authority and the vendor must comply with all applicable legal and regulatory requirements for data protection. (Information protection policies and procedures)
        - Explanation: This clause ensures that a vendor will not just protect itself against potential products or strict liability, but also will comply with legal and regulatory requirements to secure its networks.
    - Vendor should be required to disclose how it will provide assistance to 911 authorities and operators to prevent possible data breaches, and specific policies and procedures regarding how to report those breaches to the vendor. (Awareness and training)
        - Explanation: Most data breaches are the result of human error, and this clause ensures that, if an error occurs, the operators and authorities have the ability to spot those errors and to notify the vendors as soon as possible, in order to mitigate damages and reduce the risk of a full-blown data breach.
- **Detect** – Develop and implement the appropriate activities to identify the occurrence of a cybersecurity event.
    - The 911 authority should ensure that when a breach occurs, the vendor is required to immediately notify the 911 authority, quickly (within a specified time period) provide a detailed analysis of the extent of the breach, and identify the information that has been compromised. (Anomalies and events)
        - Explanation: Data breaches can occur for many different reasons. A detailed analysis will ensure that the vendor and the 911 authority can determine how to better train users and more quickly detect breaches in the future.
    - The vendor should be required to disclose the extent of its post-installation monitoring and detection processes for cybersecurity. (Security continuous monitoring/detection processes)
        - Explanation: It is up to the 911 authorities to contract for specific post-installation monitoring and detection processes, but at the very least, vendors should disclose the monitoring they provide so that 911 authorities can better understand their own obligations for ensuring cybersecurity.

[10] NSA's *Manageable Network Plan* at 17-18

[11] *See* Computer World, "Target breach happened because of a basic network segmentation error". Available at: http://www.computerworld.com/article/2487425/cybercrime-hacking/target-breach-happened-because-of-a-basic-network-segmentation-error.html

- **Respond** – Develop and implement the appropriate activities for taking action regarding a detected cybersecurity event.
    - The 911 authority should ensure that the vendor is required to disclose a plan with specific notification requirements for whenever a breach occurs. (Communications/response planning)
        - Explanation: Having a policy in place before breaches occur will ensure that breaches are fixed as quickly as possible. Some example requirements might include specifying the people responsible for identifying and communicating the breach, who should be called to report a breach, the timeline of the notification, and whether/when the public should be informed of the breach.
    - The 911 authority should ensure that after a breach, the vendor is required to disclose what changes will be made to mitigate similar breaches in the future. (Mitigation/improvements)
        - Explanation: The post-breach response analysis will play a role in determining how a vendor and the 911 authority can best mitigate and prevent breaches in the future.
- **Recover** – Develop and implement the appropriate activities to maintain plans for resilience and to restore any capabilities to services that were impaired due to a cybersecurity event.
    - After a breach occurs, the 911 authority and the vendor need to determine what steps must be taken to restore capabilities, and who is responsible for recovery. (Communications/recovery planning). These steps and the process for completing them should be specified in writing as part of the contract.
    - After a breach occurs, the vendor should be required to provide a detailed analysis of the breach response so that the vendor and the 911 authority will learn from the experience, in order to improve future responses. (Improvements)
        - Explanation: This analysis also will help the vendor and the 911 authority determine if there are additional steps that need to be taken to fully resolve the breach.

3.3.2. Two-Factor Authentication

In most circumstances, systems and networks only require a username and password to gain access. However, this common form of security has been incredibly vulnerable to hacks, breaches, and compromises because a username and password is relatively easy to obtain and fabricate.

In contrast to the single-factor, “username-and-password” form of authentication, two-factor authentication requires users to validate multiple forms of credentials before they are granted access to the system. Two-factor authentication is not a new concept; in fact, you have probably experienced it before. When your credit card machine asks you for a ZIP code, this is two-factor authentication because it requires you to have a physical token (the card itself) and a knowledge qualifier (the ZIP code associated with the card). In addition to physical tokens and knowledge qualifiers, some companies are instituting biometric information, like fingerprints or voice prints; however, this technology may be cost prohibitive at this time.

In order to ensure that 911 systems are as secure as possible, it is recommended that 911 authorities require two-factor (or multi-factor) authentication to enter their networks. Authentication factors typically include the following categories:

- Knowledge Factors (something you know) – examples: PIN, password, passphrase, answer to "secret questions", etc.
- Possession Factors (something you have) – examples: security token, smart card, etc.
- Inherence Factors (something you are) – examples: biometric data, such as fingerprints, voice recognition, retinal scan, etc.

Finally, while two-factor authentication does make networks more secure, it does not make them impenetrable to attack. Many systems implement an "account recovery" protocol that allows one to retrieve a new password in case the existing one has been forgotten. The problem with account recovery is that it likely bypasses two-factor authentication entirely. It is important that, even with two-factor authentication, account recovery questions and the emails associated with those accounts are maintained by the 911 authority.

3.3.3. Background Checks and Fingerprinting

As 911 authorities deal with the public's data, they may wish to consider requiring each person who wants to access the network to submit to a fingerprint-based background check. Background checks are routine in many industries, and they look for prior convictions or outstanding warrants that can disqualify someone from working with such networks. It has been proven time and time again that a fingerprint-based background check is the most reliable background check available.

The Federal Bureau of Investigation (FBI) is responsible for testing fingerprint-based background checks. When fingerprints are sent in, the Bureau queries its Identity History Summary, which is a list of arrest-related information associated with fingerprint submissions kept by the FBI. In some cases, the information also relates to prior federal employment, naturalization, or military service associated with the individual.

Numerous reputable firms exist that do regular, non-fingerprint-based background checks. 911 authorities are urged to work with vendors to find a contractor that can complete this research, in order to keep their networks secure.

3.3.4. Encryption and Network Management

One of the most important aspects of maintaining a secure network lies with encryption. Sending unencrypted information over the Internet is like sending a postcard in the mail: it will reach its destination, but anyone who handles the package in transit will be able to read all of the information on it. Encryption solves this problem by scrambling the message at the source, and then unscrambling it once it reaches its destination. This prevents individuals who are on the network, or lurking outside the network at some point along the transmission path, from being able to read the data.

One of the most vulnerable aspects of the network concerns user interaction. It is important to disable the ability for PSAP personnel to plug in an unauthorized universal serial bus (USB)/flash memory drive.

It is very easy for a virus or malware to infect an entire network via a USB drive. It also is suggested that the actual personal computer (PC) be locked down to prevent any unauthorized devices from being allowed on the equipment.

As a general note, jurisdictions also should update their router firmware on a regular basis. The vendor will have information on how to accomplish this, but it is a relatively easy task to ensure that one's network remains secure.

In addition to encryption, there are numerous network management practices that can keep networks safe from attack and more secure. First, it is critically important that the router's administrative username and password are changed, as the default keys for these logins are well known to attackers.

If viable, all networks should disable file and print sharing on everything other than the jurisdiction's file server (if applicable). File sharing, especially on a desktop computer, is a vulnerability whose benefit likely does not affect the everyday operations of a PSAP. By disabling this feature, the jurisdiction ensures that no one can access the network remotely and access all files available on the hard disk.

Finally, all computers should be equipped with up-to-date anti-virus and anti-spyware protection. Viruses can cause all sorts of problems for data, including erasing the data completely or sending the data to another person. Anti-virus companies stay on top of the latest-known vulnerabilities, and using their software will reduce liability in case of a breach. Additionally, anti-spyware protects against programs that exist on your computer and send all data to the attacker. Anti-spyware and anti-malware software works much like anti-virus software, and running these programs will keep the equipment safe from general attacks that affect numerous computers.

If a jurisdiction has plans to allow laptops to access the local network from home or a remote web server, or is considering such an option, it is imperative to use a virtual private network (VPN). This technology allows for point-to-point encryption and is virtually impossible to attack. This is the optimal way to ensure data security, and is relatively inexpensive. The vendor will have more information on VPNs if needed to secure the network remotely.

3.3.5. Firewalls and Firewall Management

It is important to use a firewall to protect against network vulnerabilities. On any network, there are numerous "ports" that are used to connect to the web. A properly installed firewall is the first line of defense on any network because it blocks access to ports that are not used. The only ports that should be open are the ones needed for the services to run. Firewalls on computers are different than firewalls for networks, and jurisdictions should ensure that all equipment and the network are secured via firewalls.

Firewalls should be password protected, and the password should be changed from the default password provided at deployment. Like routers, default access information for firewalls is well known to attackers, so this should be changed to ensure network security. In addition, it is suggested that routers

are configured to block pings. Pings are notifications that are essential to the Internet at large, but attackers use this capability to discover whether a particular network is exploitable.

Compliance with local, state, and/or federal cybersecurity requirement is a must. The FBI's Criminal Justice Information Services (CJIS) security policy[12] is often a requirement for law enforcement PSAPs that access criminal justice information.

If a jurisdiction does not plan to have many guest users on the network, it would be a good idea to limit and identify the IP addresses that have access. Dynamic Host Configuration Protocol (DHCP) is a network protocol that allows users to connect to networks more easily, but this function can be utilized by attackers to bypass other security measures. By manually inputting the IP addresses of the computers that will run on the network, jurisdictions close off the ability for attackers to directly access the network. Most importantly, if problems arise, disabling DHCP allows the jurisdiction to retrieve the IP addresses and network activity associated with a breach. Jurisdictions should ensure during contract negotiations that the vendor will provide the ability to disable DHCP.

3.3.6. Intrusion Prevention System

While firewalls stop traffic, and thus attacks, from entering the network via ports that normally are not used, the main port associated with web and Internet traffic (Port 80) will need to remain open for the network to communicate to the web. Therefore, if an attacker tries to use a Port 80 exploit, a firewall may be ineffective. Consequently, an intrusion prevention system (IPS) plays a key role in network security because it monitors all incoming traffic, including Port 80, for suspicious anomalies that could indicate malicious activity. While IPS is often bundled as part of router software, it is suggested that an additional IPS system be implemented because of the importance of keeping this data private and secure.

4. Conclusion

Procurement of NG911 systems is typically a rare event for most 911 entities and as a result, many people do not have direct or recent experience in contracting for these types of systems. As a result, the importance of establishing contract terms and conditions that protect the interests of the 911 entity and the local community is paramount while preparing for a procurement. This document provides the 911 community with a resource to reference during the process to ensure that aspects of procurement, such as T&Cs, SLAs, and security are adequately addressed, and the risks to the 911 authority are appropriately understood and managed.

[12] Available at: https://www.fbi.gov/about-us/cjis/cjis-security-policy-resource-center

Appendix A

A Procurement Toolkit was developed in 2009 as part of the US DOT NG911 Initiative, to provide any state and local entity with a guide and set of best practices for developing a procurement system that enables them to get the best value for their money. The Procurement Toolkit describes a typical procurement process, outlining the four phases most often needed to develop procurement documents, review processes, and a decision framework.

Phase I: Planning/Development of Bid Documents

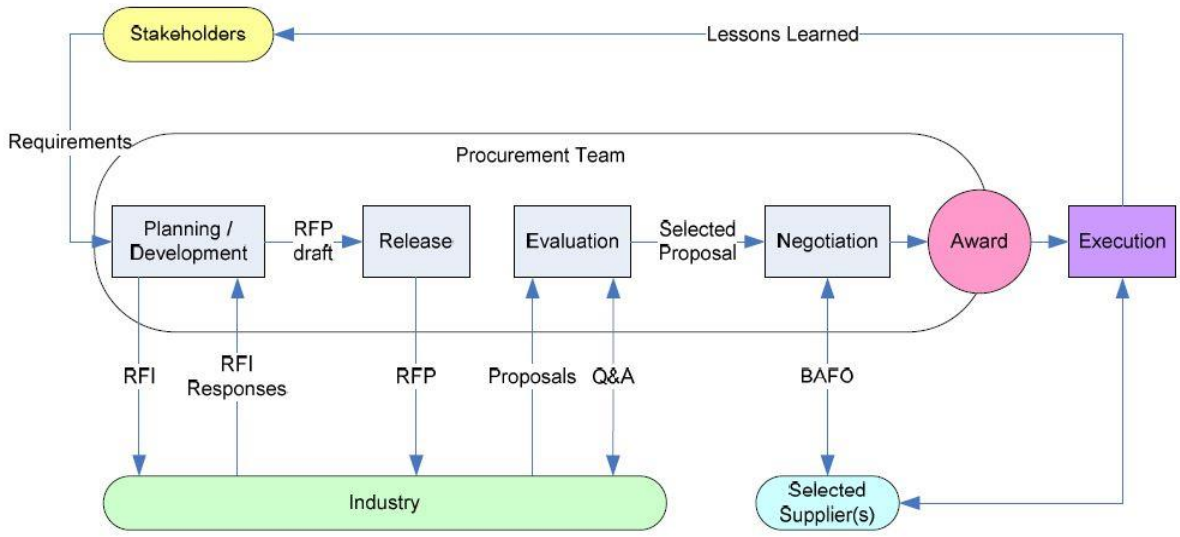
Phase II: Release the RFP/RFQ

Phase III: Evaluation of Proposals

Phase IV: Negotiation with the Selected Vendor

The flowchart below taken from the Procurement Toolkit depicts the procurement process.

Exhibit 11—Procurement Process



The entire document is located at the link below:

http://ntl.bts.gov/lib/35000/35600/35649/USDOT_NG911_Procurement_ToolKit_2009.pdf