News from the Texas Commission on
State Emergency Communications (CSEC)

Volume 1, Issue 6
November 2015

Connections

INSIDE THIS ISSUE

333 Guadalupe St.,
Suite 2-212,
Austin, Texas 78701
Telephone: 512.305.6911
Email: csecinfo@csec.texas.gov
Web: csec.texas.gov
facebook.com/TXCSEC
twitter.com/CSEC911

WE WANT TO HEAR FROM YOU

If you have story ideas for future issues of *Connections*, please send an email to:

CSECSupportTeam@mcp911.com

Call-Handling Decision Is Fast Approaching

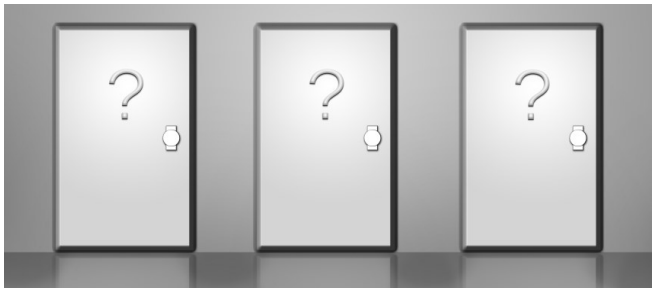
Regional Planning Commissions (RPCs) in the CSEC program are due to inform CSEC by November 20 of their preferences regarding the call-handling strategy that will be employed for the CSEC State-Level Emergency Services IP Network (ESInet) once it is fully operational.

"This is an important decision because CSEC needs this information now in order to design and build a network that supports the RPCs' desired end-state in the future," emphasizes Kelli Merriweather, CSEC Executive Director.

Public safety answering points (PSAPs) under the jurisdiction of the RPCs will be able to connect directly to the CSEC State-Level ESInet. So too will RPCs that are operating their own regional ESInets. For instance, a large RPC might wish to connect its network to the State-Level ESInet in order to execute 9-1-1 call transfers and to share vital information with other regions.

To make the most efficient and effective use of funding, the CSEC/RPC 9-1-1 Program has a distinct advantage and opportunity to realize economies of scale by leveraging shared services and costs. CSEC plans to implement an ESInet and NG9-1-1 system through competitively bid, shared-services contracts with vendors. To maintain local control, ESInet governance is being developed by RPC 9-1-1 Program staff and CSEC to ensure that all RPCs have a voice and input into the decision-making process, in a consistent and sustainable forum.

What still is to be decided is how to handle the NG9-1-1-capable call-handling equipment—also known as customer premises equipment (CPE)—that will be needed in order to accept emergency calls from the State-Level ESInet. There are three options for the RPCs to consider:



- Procure the call-handling equipment on their own
- Select equipment off an approved vendor list from CSEC
- Leverage call-handling services provided by CSEC via a cloud-based subscription model

The collective decision of the RPCs is needed so soon because planning related to legislative appropriation requests (LAR) for the FY 2018-2019 biennium already is underway, according to Susan Seet, CSEC's chief program technical officer.

"We need to have an idea of what the end-state of our network is going to look like—so we can design the NG9-1-1 system with that in mind," Seet said.

The first option is similar to the RPCs' current CPE configuration in today's 9-1-1 environment. CSEC would provision the NG9-1-1 core services version of today's selective router in its data centers across the state, and the RPCs would choose whatever vendor they wish for the call-handling equipment that supports interoperability with the State-Level ESInet.

Continued on page 4

ESInet Governance Structure Is Taking Shape

"In this model, those who use the CSEC State-Level ESInet … will change from being a passive services recipient to being an engaged stakeholder with accountability for decision-making."

– Liz Evans, KPMG

A draft version of a governance structure that would be used to make policy and operations decisions going forward regarding the CSEC State-Level Emergency Services IP Network (ESInet) is on schedule to be completed by November 20. The governance structure then will be presented to the Commission for approval during its February 2016 meeting.

The Regional Planning Commissions (RPCs) in the state of Texas nominated and selected a Governance Customer Focus Group to provide input into the governance structure through a series of Web conference calls and workshops. The structure is based in part on a governance model that KPMG, which is leading the effort, created for the Texas Department of Information Resources about a decade ago that leverages the owner/operator model, according to Liz Evans, managing director, management consulting for KPMG. The owner/operator model represents a 180-degree shift from what the RPCs have experienced in the past concerning the provisioning of 9-1-1 services.

"Fundamentally, this means that in this model, those who use the CSEC State-Level ESInet will take responsibility for ensuring that it operates properly," Evans said. "They will change from being a passive services recipient to being an engaged stakeholder with accountability for decision-making around how the operations will function."

Evans added that it is a model that's very effective with large, complex stakeholder groups, because it enables people to have a very structured interaction and involvement in the decision-making process.

"It gives them ownership of the decision and creates transparency in terms of how the decision was made," she said.

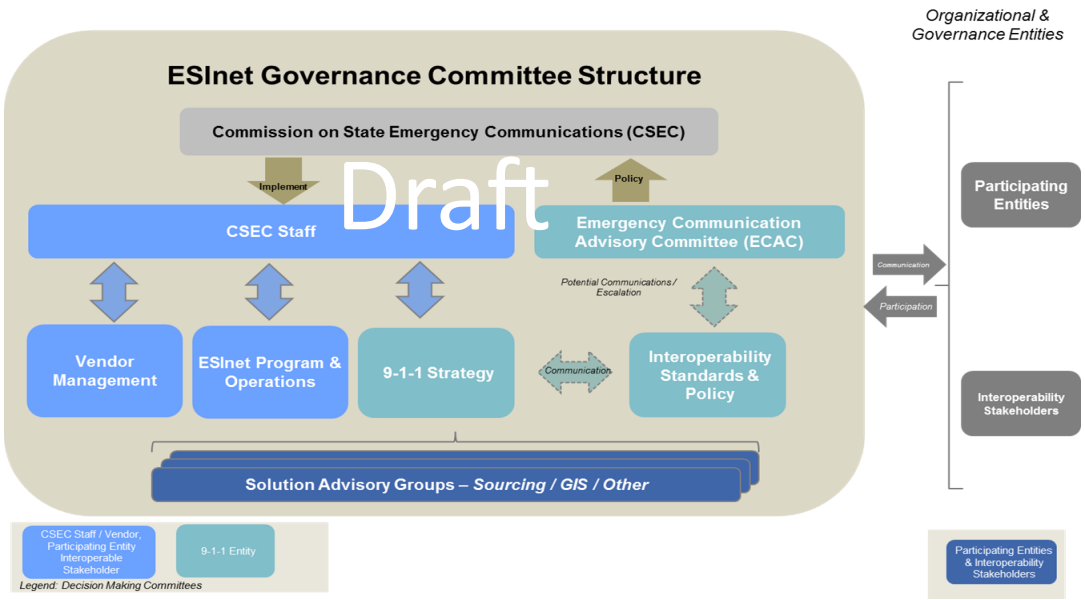
The draft governance structure identifies three stakeholder groups, as follows:

Participating Entities – An RPC or other 9-1-1 entity that uses the CSEC State-Level ESInet in order to leverage core Next Generation 9-1-1 (NG9-1-1) services.

Interoperability Stakeholder – A 9-1-1 entity or other public safety entity that interconnects with the CSEC State-Level ESInet on a network-to-network basis.

Vendor Management – Management of all carriers and suppliers utilized to operate the CSEC State-Level ESInet and its functional elements. (CSEC will provide system requirements for participating entities to provide to their vendors for connectivity to the network.)

Continued on page 4



GIS data scrubbing needs to be a 'ritual process'

The quality of Geographic Information System (GIS) data always has been important, as law enforcement, the fire service and emergency medical services all have leveraged such data to support their missions for years. However, GIS data will play an even more critical role in Next Generation 9-1-1 (NG9-1-1) environments because it will be the primary tool used to locate emergency callers regardless of the device they use to make the call.

For that reason, the National Emergency Number Association (NENA) has recommended that a 98-percent match rate exists between a PSAP's GIS data and the Master Street Address Guide (MSAG) and the Automatic Location Identification (ALI) databases before the GIS data is used to locate emergency callers.

Previously, that was a big problem for the Rio Grande Council of Governments (RGCOG), which encompasses Brewster, Jeff Davis, Presidio, Hudspeth and Culberson counties.

"When I went to work for the council in 2009, the error rate stood at about 15 percent," said Catherine Crumpton, an RGCOG GIS coordinator. "We were in the high-risk group."

Aarón Burciaga, the RGCOG's other GIS coordinator, who has been on the job for about a decade, concurred: "When I started in 2006, the data was in dire shape."

Crumpton and Burciaga decided to do something about that, and the results have been nothing short of amazing: currently, the RGCOG's data quality is such that the current MSAG/ALI match rate is between 98 and 99 percent.

It wasn't easy given the limited resources that Crumpton and Burciaga have at their disposal.

"We're a very small COG, so we wear a lot of hats," Crumpton said. "But accuracy in addressing and mapping is the number-one priority, because no one gets saved if the information isn't good. You have to be persistent."

Burciaga added that data scrubbing needs to be a "ritual process." Part of the ritual in the beginning was to get to the office an hour or two early each day.

"I arrived early in order to make phone calls so that I could confirm addresses," he said. "You have to catch people before they leave for work. An hour or two makes a big difference."

Crumpton and Burciaga aren't doing it totally on their own. For example, various county and municipal agencies—from the tax assessor and code enforcement department to the department of motor vehicles and myriad utilities—are doing their part.

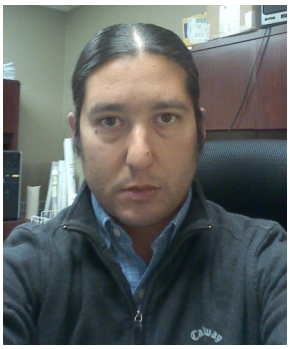
"If someone applies for a building permit, for instance, they will be sent to us first so that we can reconcile the address," Crumpton said.

She added that individual citizens also get into the act on a regular basis.

"Years ago, the RGCOG used contractors to assist with the addressing and—per our instructions—they used mile markers because we're very rural, which is not the preferred method now," Crumpton said. "So, residents often reach out to us when they think that they might not have a good address—they want to make sure they're rescued."

Ensuring GIS data quality is analogous to owning a house—regular ongoing maintenance is far less onerous than allowing the building to fall into disrepair and then fixing the problem(s). In this regard, having an ownership mentality is a real plus, according to Burciaga.

"We're the 9-1-1 authority, and this is what we do," he said. "We have to act in a very specific way—we are very detail oriented—we bleed 9-1-1."■



"We're the 9-1-1 authority and this is what we do. We have to act in a very specific way—we are very detail oriented—we bleed 9-1-1."

– Aarón Burciaga,

"We're a very small COG, so we wear a lot of hats. But accuracy in addressing and mapping is the number-one priority, because no one gets saved if the information isn't good."

– Catherine Crumpton, RGCOG

Call-Handling Decision Is Fast Approaching

"We need to have an idea of what the end-state of our network is going to look like—so we can design the NG9-1-1 system with that in mind."

– Susan Seet, CSEC

Continued from page 1

The upside to this approach is that RPCs would have total control over the provisioning of their CPE. The downside is that RPCs also would bear the full responsibility of ensuring cybersecurity and interoperability, and executing the necessary and inevitable hardware and software refreshes.

The second option would require RPCs to relinquish some control, but also removes some of the responsibilities associated with deploying the CPE. RPCs would select from a list of CSEC-approved options that have passed tests conducted by the Texas A&M University (TAMU) test lab. The upside to this approach is that the procurement would be done by CSEC and there would be no interoperability issues. The downside is that the TAMU test lab will not exist into perpetuity, so future software revisions for selected equipment will require validation of interoperability prior to deployment.

The third option calls for CSEC to provision and manage everything needed to interconnect with the State-Level ESInet and leverage its services from end to end, all the way to the desktop equipment that will be used by 9-1-1 telecommunicators. In this model, the RPCs would work collaboratively with the PSAPs in their respective jurisdictions to identify the features and functionalities of their ideal CPE, utilizing the ESInet governance structure.

With CPE requirements from RPCs, CSEC would procure CPE from two to four vendors that meet the RPC requirements, with the number hinging on budgetary factors. The call-handling functionality then would be made available as a cloud-based service.

There are several pros and cons to this approach. State procurement rules require CSEC to acquire the CPE via competitive bidding. Consequently, there is no guarantee that RPCs' favorite CPE manufacturer or model would be selected. However, the burden of deployment, interoperability, compatibility with NENA's i3 architecture, and system refreshes all would be borne by CSEC, not the RPCs.

"We want the RPCs to have a voice and a choice as to how the CSEC State-Level ESInet is rolled out," Merriweather said. "We need our participating RPC 9-1-1 Programs to make decisions and provide direct input via the new governance structure so we are all successful in deploying NG9-1-1 in Texas."■

ESInet Governance Structure Is Taking Shape

"We've tried to create a structure that is both flexible and scalable."

– Liz Evans, KPMG

Continued from page 2

Four committees are being considered as part of the governance structure for the State-Level ESInet. These committees—which always will have RPC representation— would be as follows:

Vendor Management – Provides oversight of third-party vendors—i.e., system integrators, network providers and application developers—contributing to the State-Level ESInet, to ensure that financial and contractual obligations are met.

ESInet Program & Operations Management – Provides oversight of the State-Level ESInet, with a focus on day-to-day management, particularly in the areas of network performance, call-handling, cybersecurity, and technology refreshes.

Interoperability Standards & Operations Management – Provides guidance concerning interoperability standards and procedures required to support the State-Level ESInet, to ensure that each entity needing to connect to the network is able to do so, and that voice and data traffic flows between the entities seamlessly and without issue.

9-1-1 Strategy – Provides overarching oversight and drives the evolution of the State-Level ESInet.

In addition, **Solution Advisory Groups** will be formed as needed to support the committees when policy, operations, fiscal and technology issues or opportunities occur.

"We've tried to create a structure that is both flexible and scalable," Evans said.■

Border Control Function is ESInet's Safety Net

One of the key components of any Next Generation 9-1-1 (NG9-1-1) network is the Border Control Function (BCF), which is a term coined by the National Emergency Number Association (NENA) for security at the edge of the network.

"In the information technology world, they've dealt with firewalls and virtual private network devices for years, and in the telecommunications world they've dealt with session border controllers," said Milton Schober, a communications consultant for Mission Critical Partners, Inc. (MCP), a public safety communications consulting firm that is supporting CSEC in its development of the State-Level Emergency Communications Internet Protocol (IP) Network, or ESInet.

"What NENA did was roll up all those edge-security functions into one term, the BCF."

Of the three, the session border controller arguably is the most critical, because it is designed specifically to handle streaming traffic—and because an ESInet is IP-based, it will be used to transport streaming voice as well as video. As a result, network administrators will need to start thinking a little differently, according to Schober.

"Handling streaming traffic takes more horsepower than other kinds of data traffic," he said. "There is more processing involved and it has to occur faster, because if you lose packets in that stream, you lose the intelligibility of the voice—words will go missing—or the video will be pixilated."

The BCF will reside at the edge of the CSEC State-Level ESInet, as well as at the edge of the Regional Planning Commission (RPC), public safety answering point (PSAP), and other 9-1-1 entity networks that interconnect to it.

The BCF protects all of these networks by ensuring that any traffic going into them not only is legitimate, but also is intended for the receiving network.

"In the legacy circuit-switched environment, network connections were hard-wired private lines, so security wasn't an issue," Schober said. "Things are very different in an IP environment—security is a very big deal due to the anywhere-to-anywhere nature of the network."

According to Schober, even though the connections between CSEC's network and the other networks will be private, there still is the potential for unwanted traffic to accidentally make its way into these networks, primarily through malware attacks, accidental misprovisioning of network connectivity, or other failures in the network.

"Malicious traffic tends to have a signature, almost like a fingerprint. The BCF would recognize that and prevent it from going through."

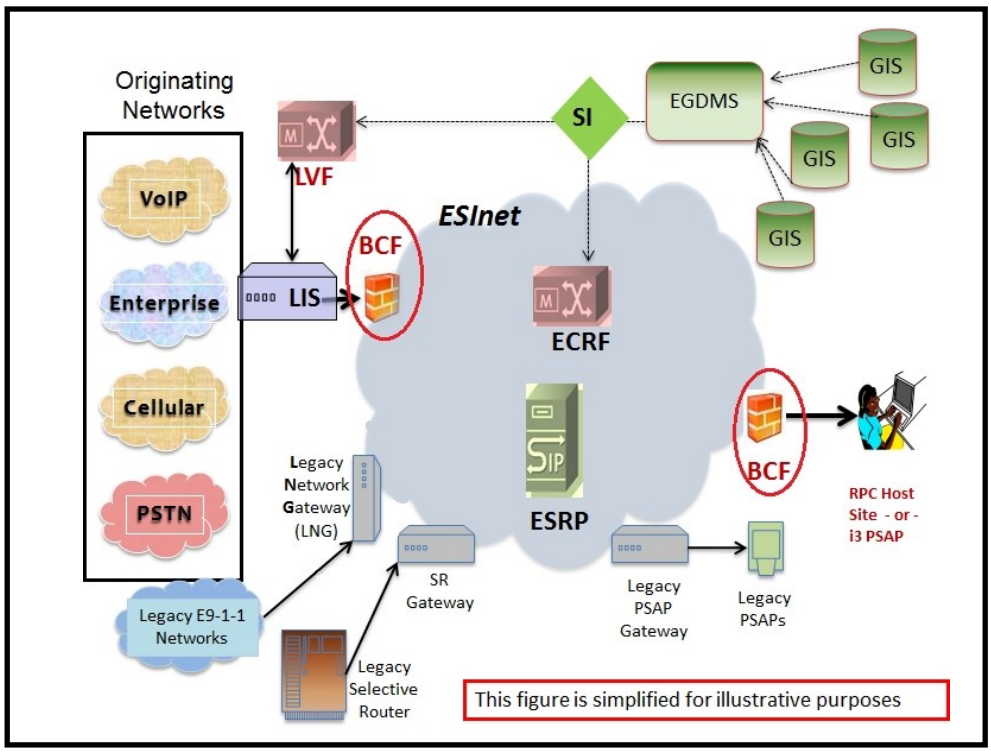
– Milton Schober, MCP

"The BCF is the safety net designed to prevent that from happening," he said.

A key element of the BCF's ability to protect networks is its built-in intrusion-detection/–prevention functions that would identify and quarantine any malicious content.

"Malicious traffic tends to have a signature, almost like a fingerprint," Schober said. "The BCF would recognize that and prevent it from going through."

The BCF employed by CSEC for the State-Level ESInet will be a carrier-grade system deployed at the network core; in contrast, the BCFs that will reside at each RPC will be far smaller and simpler to provision. ■



This diagram shows the relative positioning of the BCF in a NG9-1-1 network configuration.