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

Volume 1, Issue 4
June 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

BVCOG Leads the Way on Text-to-9-1-1

The text-to-9-1-1 pilot project currently being conducted by the Brazos Valley Council of Governments (BVCOG) is progressing very well, so much so that the four public safety answering points (PSAPs) participating in the pilot were expected to be ready to field 9-1-1 texts beginning in mid-June.

This will follow a period, which was scheduled to begin on May 25, during which text-to-911 calls will be simulated to ensure that all systems are functioning properly.

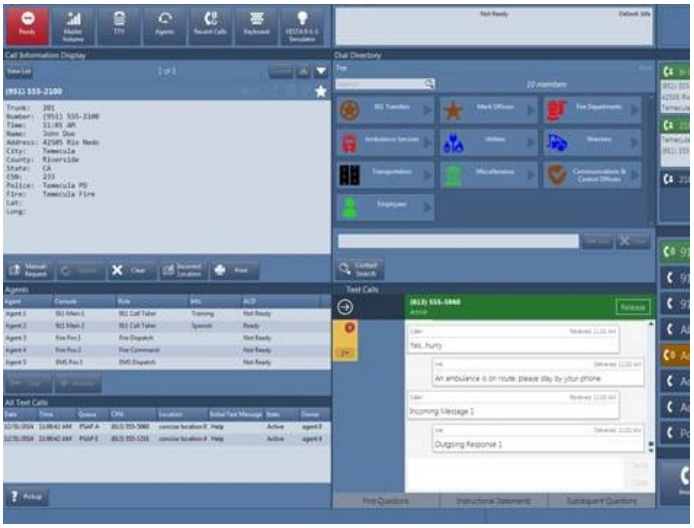
However, BVCOG will wait until September before informing the public about this vital new service, according to Anita Pitt, BVCOG's program manager.

"We want this to be thoroughly tested before the public starts to use it," Pitt said. "So, we're going to test calls over the summer," Pitt said. "Then we'll do a public education campaign."

CSEC Executive Director Kelli Merriweather thanked Pitt for her efforts as a NG9-1-1 trailblazer in taking on this vital pilot project.

"Her efforts are making text to 9-1-1 a reality in the state of Texas," Merriweather said

Pitt added that after an initial period of concern, telecommunicators in BVCOG's PSAPs now are excited about text-to-9-1-1.



Example of an integrated telecommunicator screen; the 9-1-1 text appears in the lower right corner.

"They were most worried about having to deal with two screens, one for text calls and one for voice calls," Pitt said. "But Airbus came up with a way to integrate the screens."

Instead of having to use a separate screen, the 9-1-1 text will appear on their regular screen—just the way a voice call comes in—and they will be able to handle it the same way, including transferring the 9-1-1 text to another PSAP.

Other upgrades include expanding the Automatic Location Identification (ALI) circuit—which previously provided 56 kbps bandwidth—to a full T1 line, and upgrading the ALI router to a Cisco 1921. BVCOG will use the Message Session Relay Protocol (MSRP) to deliver 9-1-1 texts to the PSAPs.

The utilization of MSRP during the pilot project is significant, Pitt said.

"It represents the first implementation of Next Generation 9-1-1 in the state," she said. "The pilot will provide a beta test to see how Geographic Information System (GIS) data can be used to locate callers."

Pitt added that she's excited that BVCOG soon will be able to provide this vital service to citizens in its jurisdiction.

"When we first started talking about this several years ago, it seemed so futuristic," she said. "So seeing it come to fruition is very exciting."■

Lab Tests Focus on Gateways, Geospatial Routing

Laboratory testing of the transitional network elements that will be required during the early stages of Next Generation 9-1-1 (NG9-1-1) deployment in the state of Texas will begin this summer.

The laboratory environment—the first of its kind in the nation—leverages the combined test laboratories of the Texas Department of Information Resources (DIR) Data Center Services (DCS) and Texas A&M University's Internet2 Technology Evaluation Center (ITEC).

The lab will be used to build and test a complete, virtual NG9-1-1 system from end to end.

"We have to be ready for the day when everything is Internet Protocol (IP)-based, which is what this testing is all about.
—Kevin Rohrer, CSEC

"The carriers are moving away from their legacy switches, and we have to be ready for the day when everything is Internet Protocol (IP)-based, which is what this testing is all about," said Kevin Rohrer, CSEC Network Program Manager.

The lab has created tremendous interest from NG9-1-1 systems and component manufacturers, which are lining up to donate their hardware/software to the effort, as follows:

- The Texas Department of Information Resources—backbone network
- CenturyLink—selective routers
- Intrado—Automatic Location Identification/Location Validation Function (ALI/LVF)
- GeoComm—Enterprise Geospatial Database Management System (EGDMS)

CSEC is undertaking this intensive testing program with its system integrator—Capgemini—and an independent testing services provider, in order to build the very best-of-breed NG9-1-1 system for the Regional Planning Commissions (RPCs) that the CSEC program supports. The testing will inform CSEC on the very best network design and National Emergency Number Association (NENA) i3-capable systems and software.

The laboratory testing consists of three projects, as follows:

- The first project will test the functionality of the Legacy Network Gateway (LNG) and Legacy Selective Router Gateway (LSRG), with an emphasis on identifying risks and issues associated with call traffic migration and call routing. The LNG and LSRG are elements of the i3 architecture.
- The second project will test call-routing equipment hardware and software, including the Emergency Services Routing Proxy (ESRP), Policy Routing Function (PRF), Emergency Call-Routing Function (ECRF), Legacy PSAP Gateway (LPG) and the Location Validation Function (LVF). Like the LNG and LSRG referenced above, all are elements of the i3 architecture.
- The third project will test i3-compliant customer premises equipment (CPE) hardware and software used to support call-handling functions.

The tests as a whole are intended to ensure that a 9-1-1 call can be routed to the appropriate PSAP, using Geographic Information System (GIS) data, with the caller's location embedded. In addition, the tests will help CSEC determine the optimal design for NG9-1-1 services in Texas.■

EGDMS to Play a Vital Role in NG9-1-1

The Enterprise Geospatial Database Management System (EGDMS) is a repository of Geographic Information System (GIS) data that has been generated by Regional Planning Commissions (RPCs) in the State of Texas. As such, it will play an extremely important role in the state's migration to Next Generation 9-1-1 (NG9-1-1).

The EGDMS resides in two data centers operated by GeoComm, which is the GIS software and related services provider that will operate the system. GeoComm was selected by a customer focus group comprised entirely of Regional Planning Commission (RPC) representatives.

Continued on page 4

NG9-1-1 Cybersecurity Plan Takes Shape

Though Emergency Services Internet Protocol (IP) Networks (ESInets) are closed, private networks, they still will be vulnerable to the same cyber attacks that threaten all IP-based networks. In fact, the CSEC State-level ESInet will be under constant threat from a variety of internal and external sources.

Consequently, an IP-based Next Generation 9-1-1 (NG9-1-1) network will require a much greater focus on network security.

For this reason, CSEC has developed, with support from its system integrator, Capgemini, the State-level ESInet Cybersecurity Plan. The Plan builds upon the CSEC State-level ESInet Security Policy, which was adopted by the Commission on March 10, 2015. The Policy was developed in a partnership between CSEC, a subcommittee of Texas 9-1-1 entity stakeholders, industry vendors, and AT&T.

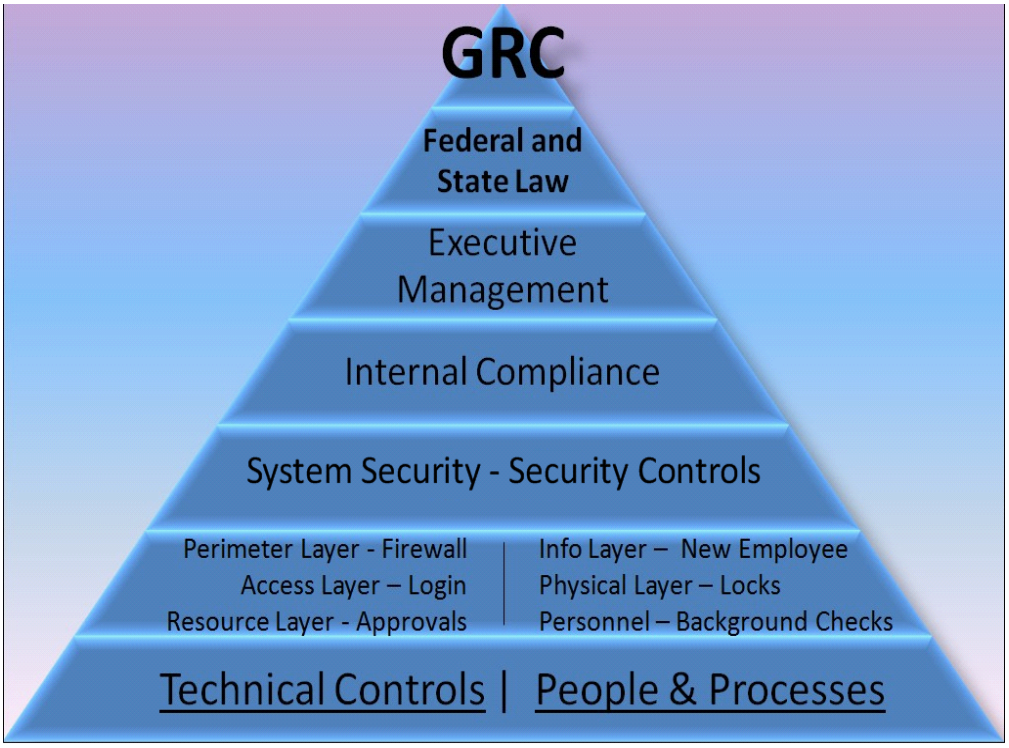
Although cyber risks may not be completely avoidable, the Plan establishes a strategy for minimizing the risk of unauthorized access to the systems and data of organizations that will connect to CSEC's State-level ESInet.

A key element of the Plan is the Governance, Regulatory and Compliance (GRC) stack, which is illustrated in the figure below. The GRC stack forms an ecosystem that coordinates activities and information across all areas of the enterprise using a single consolidated framework.

In addition, the Plan describes a plethora of tools that can be used to ensure a secure network environment. These tools include the following:

- **Firewalls—**A firewall is a network security system that controls incoming and outgoing network traffic based on an applied rule set. A firewall establishes a barrier between a trusted, secure internal network and another network (i.e., the Internet) that is assumed not to be secure or trusted.
- **Intrusion Detection/Prevention Systems—**They are network security appliances that monitor and proact-

Continued on page 4



Governance, Regulatory and Compliance (GRC) stack.

Though ESInets are closed, private networks, they still will be vulnerable to the same cyber attacks that threaten all IP-based networks. In fact, the CSEC State-level ESInet will be under constant threat from a variety of internal and external sources.

The State-level ESInet Cybersecurity Plan establishes a strategy for minimizing the risk of unauthorized access to the systems and data of organizations that will connect to CSEC's State-level ESInet.

Cybersecurity Plan

Continued from page 3

ively prevent network traffic from performing malicious activity. Additionally, the system will log the activity and report it to a system administrator for analysis.

- **Network Monitoring Tools—**They are used to monitor, analyze, diagnose and troubleshoot issues that could affect the operational integrity of the ESInet.

In addition to the network-based protections described above, there are several operational best practices that, if followed on a regular basis, will enhance the security of CSEC's State-level ESInet. These include the following:

- Change network log-in passwords on a regular basis.
- Ensure that personnel have the level of network access that is appropriate for their role.
- Instruct personnel not to loan their passwords, even to trusted colleagues.

Other recommendations identified in the plan include the following:

- Appointment of a program-level Information Security Officer to develop, maintain and enforce the policies established in the Plan.
- Selection and implementation of a risk-management framework that supports the security controls of the GRC stack (which is illustrated on page 3).
- Acquisition of a single-sign-on (SSO) access control manager to authenticate and authorize ESInet users. In accordance with NENA standards, the SSO implementation should leverage the Security Assertion Markup Language (SAML) protocol.
- Acquisition of an industry-standard tool to ensure that network access for users that have left the organization has been terminated across the enterprise.■

EGDMS to Play Vital Role

Continued from page 2

GeoComm accepts and coalesces the GIS data and performs quality assurance/quality control (QA/QC) checks. The GIS data contained in the EGDMS must match the legacy Automatic Location Identification (ALI) and Master Street Address Guide (MSAG) data at a rate of 98 percent, which is the minimum threshold established by the National Emergency Number Association (NENA) before GIS data can be used to locate emergency callers.

The 98-percent match rate between the databases also must be achieved before an RPC can utilize CSEC's State-level Emergency Services Internet Protocol (IP) Network, or ESInet.

The match rate must be achieved for each of the following categories:

- MSAG high range to road centerlines
- MSAG low range to road centerlines
- ALI to road centerlines
- ALI to site structure address points

Once the QA/QC check is complete, GeoComm will pass the accurate data into CSEC's EGDMS, and will refer the inaccurate data back to the RPCs, which will correct the discrepancies. GeoComm then will perform another QA/QC check on the corrected data. This will continue until the 98-percent match rate is achieved.

Currently, the data only will be used to validate incoming service orders to the ALI/LVF (location validation function), said Monica Watt, CSEC data quality manager.

"However, if the data is used for NG9-1-1 call routing and the discrepancies aren't resolved, then this could result in misrouted calls or a 'no records found' indication," Watt said. "

Watt acknowledged the efforts of the Rio Grande Council of Governments (RGCOG), the smallest RPC in Texas. So far, RGCOG has met the 98-percent match rate requirement for two of the categories and is close for the other two.

"They have achieved the highest data quality of any RPC in the state," Watt said.■