GRABBING GOVERNMENT WORK

BY CURT HARLER

"Doing project work is like hunting for squirrel. You eat one day but are hungry the next," said Michael S. Rogers, PSP, CPP, and chief executive officer of Securityhunter, Baltimore, MD. Securityhunter was the #1 ranked systems integrator in SD&I's Fast50 program chronicling America's Fastest Growing Systems Integrators

http://www.securityinfowatch.com/article/10635998/

A lot is changing in the federal government security market. If you are not already a player in this space, you'd better do a lot of homework before you dive in. However, there are good opportunities for qualified players to make a living in this changing field.

"The access control business, as we know it, will be history in the next three years," said Jorge G. Lozano, president and chief executive officer of Condortech Services (CTS), Springfield, Va. "I see more consolidation because of cloud computing and software as a service," Lozano continued.

Condortech promotes itself as the "best ally against crime and terrorism." It was started in 1988 by three partners with a background in access control and databases who saw a chance to serve a market. Lozano purchased the market area and continued to grow the business. "After 9/11, we dedicated ourselves to the Federal market and understanding the needs and problems of the government," Lozano said.

"The future is written on the wall for our industry," Lozano continued. "People demand information. When you are using access control to protect a facility, an infrastructure or a border, you have to send lots and lots of data to the command center."

Today, he sees threats from three areas: traditional terrorism or criminal activity, cyber-terrorism and narco-terrorism. Of the three, he fears the latter most. Narco-terrorists simply have no boundaries to what they will do (see related story on page 52).

He said it is critical to be able to protect cameras and access control systems from cyber attacks. "Somebody can remove the reader and you are stuck," he noted. "Those are the kinds of challenges we need to consider."

"You also have to understand interoperability. The government wants everyone to work together since they've invested so much money in the infrastructure already," Lozano said.

Working into government forays

Michael and Nancy Rogers spent many years scoping out the government sector before Securityhunter Inc. got its first big break. They decided to 'shoot the moon' and it worked.

"Doing project work is like hunting for squirrel. You eat one day but are hungry the next," said Michael S. Rogers, PSP, CPP, and chief executive officer of Securityhunter, Baltimore, Md. Securityhunter was the #1 ranked systems integrator in SD&I's Fast50 program chronicling America's Fastest Growing Systems Integrators *http://www.securityinfowatch.com/article/10635998/.*

In Washington, a typical small security firm bids on a small business set-aside. If they win, they get a little project. Next month, they need

another. And so it goes. Not for Securityhunter.

"We won a GSA schedule with a Blanket Purchase Agreement (BPA)," Rogers said. While they lost their competitive advantage against the big guys—under a BPA there are no nods to size—they gained a $500 million purchase award. That does not mean they got a $500 million contract. Rather, it means they have access to compete on $500 million in jobs.

The next step with a BPA is two-part, just like launching a rocket. One agency must have money in its budget to spend. A contract person must approve the spending. Both people have to "turn the key" before the job launches. That happened many times for Securityhunter at sites from the Pentagon to the FAA to USDA.

However you get the business, winning the job is not the only thing that needs to be done. One must have the deliverables. Lozano rues the fact that the security industry did not get deeply involved in the data transmission standards discussion. "This allowed other players, with great IT solutions, to come in, but they did not have the understanding, like we do, of physical security, like protecting a perimeter," he said.

An IT company does not understand where the electronic fences need to be positioned. Transfer of data, audio and video to command centers needs to be instant across a variety of companies' products. CTS has made a good living out of capturing such data instantly and transferring it immediately to the first responders.

Knowing integration is a good thing

"It's not just a door you are securing. You need to consider how that door is integrated to the entire area," Lozano said.

That experience and vision came only with time both for Lozano and for Rogers. Both have worked in the federal space for several years and worked hard at it. Their efforts have been rewarded as their companies made serious headway into the market space.

Early on in the federal sector, the major players like ADT and Wells Fargo did a great job of providing access control. However, in 2004 President Bush sent down a mandate outlining the technical requirements that NIST soon would codify.

GSA and the Department of Defense led a call for a common access card (CAC) and smart card for security. Those cards emerged from the mandate. "There was a mandate for certificates and transmission of data for the cards," Lozano said. Whatever the brand name of the product, the government demanded it work quickly and accurately.

"A major challenge we have as an industry is how we are going to protect those control units from cyber attacks," Lozano stated.

Homeland security demands that systems be more interoperable and talk to one another, Lozano noted. Ability to provide that kind of service is a make-or-break for integrators and security centers.

"You have to be able to send lots of data to those command centers. Some of today's devices do not send data fast enough," Lozano stated.

The up-time needs to be 99.999 percent with full redundancy—not 99 percent, Lozano said. That is a huge difference. And it applies whether you are the Virginia Transportation Department using cameras to locate people and problems on the highways or an agency protecting a government installation.

Energy efficiency is mandated. Controllers have to be energy efficient. Data centers have to offer full disaster recovery. CTS's D.C.-area data center is backed up in Washington State.

Nothing is too tough for an enterprising integrator. However, Lozano said that succeeding in the federal market space will be a tough row for a newcomer to hoe.

"My frank opinion is that it is too late for someone to get into the government security business," Lozano said. "I saw a rush of security companies after 9/11 and I've seen most of them go out of business."

There are plenty of incentives for small businesses, women, minorities and military. "If you understand the market, and you have the technology, there are a lot of holes you can fill. There is a niche there."

"For someone in integration, it's going to be tough," Lozano continued. He said it will be difficult to learn enough fast enough and survive the infighting caused by budget cuts. He has seen a lot of defense contractors coming back

from Iraq and Afghanistan who now compete with security firms.

Rogers would put it differently. "It's open to everybody. But it takes a long time to get established," he said. "To be a chess master takes 10 years. Most guys quit after two or three years. It took me 10 years in the federal space to know what I am doing."

He compares gaining a toehold in the federal sector to doing a jigsaw puzzle without having the picture. "It sounds simple," he said, "but there is nothing simple about it."

Getting started successfully?

Do the due diligence and upfront work with fervor. "It is a great challenge. For those who are new, be aware that the economy is tough. You have to think before you open a new business. There are many challenges. It is not a lost cause. You have to know the market and the demands of the technology like fast video and fast audio," Lozano continued. Rapid deployment is critical, he added.

"There is a lot more that needs to be done if you understand the technology," Lozano said. Know standards like 800-116 for physical access control systems.

"Learn the industry well. It is not enough to understand security. You have to know the genesis of security in order to perform well in this industry," Lozano advised.

"You can't just put your toe in it," concurred Rogers. He had an office in the USDA building so he could be close to the customer. Rogers carefully nurtured relationships and won the contract. "The big companies followed our lead," he said. Even after beating a huge operation like Johnson Controls, Securityhunter and Johnson Controls Security Systems became great partners, combining to benefit mutually on government work.

Despite the steep learning curve, both Rogers and Lozano love working in the Capital. "Washington is the City of Power. You get to understand what is going on inside the Beltway," Lozano concluded.