Solving the dilemma that is federal funding

Despite millions of dollars in allocations, the public sector has just begun to do what needs to be done to boost security.

BY JOANNE FREDRICK

O n paper, the numbers seem impressive. Millions of dollars being allocated and spent for homeland security-related protection of airports, seaports, rail lines and critical infrastructure such as chemical, water and power plants. However, the reality for those who must implement government-mandated security programs is that grants often cover just a portion of the cost of risk assessment and implementation, leaving little if nothing toward operation and maintenance.

“‘What we’re doing in allocating funds is putting programs in place. But we need to fund operating expenses as well as the installation expense.” — Roy Bordes

What’s happening, said Bordes, is “we’re putting in security measures that for the first two to three years are workable.” But then there arises the issue of upgrades and maintenance. “We’re creating a monster that needs to be fed,” said Bordes about the Transportation Security Administration-related projects.

While the American Public Transportation Association lauded the Department of Homeland Security’s recent allocation of $135 million for transit security, the reality of covering the security needs for rail, bus and ferry travel, according to a prepared statement from APTA President William Millar, is a $6-billion-plus price tag.

That $6 billion breaks down to $5.2 billion for capital expenditures and $800 million for operational security investments.

Similarly, said Jeff Brown, director of ports for Ross & Baruzzi, a design, engineering and security consulting firm, the estimated cost for the Coast Guard for funding all sea-port-related projects is $9 billion.

Meanwhile, the Port Security Grant Program had given out $565 million for 1,200 projects through four rounds of funding, according to written testimony in February to the Senate Committee on Commerce, Science & Transportation from Jean Godwin, executive vice president and general counsel for the American Association of Port Authorities.

According to Godwin’s statement, “only one-sixth of all (security) projects have been funded, showing the great need for this program.”

The ports are struggling, said Susan Monteverde, vice president-government relations for the AAPA. To pay for security projects beyond the grant monies received to cover infrastructure costs, she said, most ports are taking money from funds earmarked for other activities. And while all seaports are compliant with the Maritime Transportation Security Act’s baseline requirements, Monteverde said they are now looking at reaching that next level of security.

Brown, who is the former security director at Port Everglades in Florida, said ports are challenged as they comply with the MTSA, “because ports weren’t designed with security in mind.”

Measures to improve security have ranged from setting up gates to more sophisticated access control and credential measures, he said.

Bordes noted that the initial focus on securing airports and screening airline passengers and baggage has been 50 percent to 100 percent completed, with some “very large holes” still existing on securing cargo areas and screening passengers and equipment for private aircraft.

The ports, meanwhile, are just getting under way, he said. “The port issue is an extremely expensive one,” said Bordes, echoing Brown’s comments on the difficulty of securing large, open, busy areas involving thousands of containers of cargo.

“The ports are still receiving a lot of money because there’s a lot of work to be done there,” said Tony Padilla, chief technology officer for Stanley Security Systems.

As a result of all the activity related to ports and now ground transportation such as rail, Padilla said the security consulting community is among the busiest, providing risk assessments and helping write grants to secure federal funds.

John Phillipi, director of security consulting at Ross & Baruzzi, concurred “there has been a benefit for the security industry” with homeland security-related projects. “The trend is definitely upward.”

Even though installations are the focus of security projects, ahead of them comes the critical risk and needs analysis followed by the grant-writing process, he said. Because there is a finite amount of money for projects, Phillipi said securing the grant is key. “We document the vulnerability assessment, and if you can communicate that well, you can get the money,” he said.

However, noted Bordes, many of these are private facilities whose security won’t be 100 percent funded by the government, but rather will require a public/private joint venture. “The best situation is to provide tax credits for upgrading these facilities,” commented Bordes. “We need to work out a way to protect them.”

The government, he said, is also channeling money toward critical infrastructure, ranging from utilities to watersheds. All of these, he said, will require fences and cameras to make them more secure.

The ones who are doing well are in new technologies like digital video analysis,” he said. Not only does such technology “give eyes and ears” to clients, he said, but also they reduce operational costs, which aren’t covered by grants.

AAPA’s Monteverde said ports are among those organizations looking to employ the next generation of intelligent security technology. Money initially was spent on the basics, she said, such as lighting, sensors, access control and gates. “But now we’re moving toward technologies that provide other efficiencies in the ports,” she said.

Brown of Ross & Baruzzi said the offset for the costs of personnel and maintenance, port clients are going to intelligent video systems. He cited one client that has been able to do away with having someone monitor a console and has put the monitoring capabilities into the hands of police, who can view video from their vehicles.

“Those things do come with more cost,” noted Brown, “but it is an enhancement to the security system.”

When it comes to spending the grant monies allocated to projects for airports, seaports and now rail systems, Phillipi said most projects involve CCTV, access control via card systems or guards and other perimeter, intrusion prevention-based measures.

“Where (integrators) should focus is where the federal government will spend their money,” said Padilla. He pointed to the government’s smart card program, which will not only impact government installations, but any private sector companies that do business with government entities.

The government, he said, is also channeling money toward critical infrastructure, ranging from utilities to watersheds. All of these, he said, will require fences and cameras to make them more secure.

However, noted Bordes, many of these are private facilities whose security won’t be 100 percent funded by the government, but rather will require a public/private joint venture. “The best situation is to provide tax credits for upgrading these facilities,” commented Bordes. “We need to work out a way to protect them.”

The government is, he said, “going to look at all of these things and make sure that they are being done in the most effective way.”

Phillipi added the bottom line is that “the more security is put into place, the more the public sees it as being in their best interest.”

The issue will likely continue as the federal government deals with budget cuts, Bordes added. “The only way to fix it is to find new sources of funding.”