

CQ HOMELAND SECURITY – INTELLIGENCE

March 26, 2004 – 7:11 p.m.

Federal 'Red Teams' to Probe Private Infrastructure for Security Weaknesses

By Tim Starks, CQ Staff

Infrastructure protection officials at the Homeland Security Department plan to deploy teams of security experts to probe ports, computer systems and other components of the nation's critical infrastructure to find weaknesses that could be exploited by terrorists and other nefarious forces.

DHS' Information Analysis and Infrastructure Protection Directorate included funding for the so-called red teams in its fiscal 2005 budget request.

And although outside experts almost unanimously praised the concept of running red team drills against public and private critical infrastructure, some questioned whether IAIP is ready for that kind of role.

Several federal departments and agencies have long used red teams to test security. The departments of Defense and Energy, for example, have deployed Special Forces units to probe security at military installations and sites in the nuclear weapons complex.

And the Federal Aviation Administration has used red teams to see whether weapons can be smuggled onto commercial aircraft.

According to budget documents and information provided by a DHS official who spoke on condition of anonymity, the IAIP red teams would be deployed to test physical and cyber security in the private sector as well as the security systems used by other components of the Homeland Security Department.

The National Strategy for the Physical Protection of Critical Infrastructure and Key Assets, published by the White House in February 2003, calls on DHS to use red teams to "evaluate preparedness" based on an "accurate assessment of national-level critical assets, systems, and functions."

But both the fiscal 2005 budget documents and the homeland security official withheld some key details about the teams.

Funding for the program was included as part of the \$19 million request for IAIP's Competitive Analysis and Evaluation program, which also include tabletop exercises and other methods for gauging the division's performance.

The IAIP budget justification submitted to Congress lists a number of participants in the red team initiative, including contractors, think tanks, the Pentagon and other experts, but neither that document nor the DHS official would reveal specific budget numbers,

personnel levels or time frames for deployment. The official said personnel levels are expected to fluctuate greatly.

Several members of congressional oversight committees and subcommittees, and their staffs, said they had no specifics on the red teams either.

Target Rich Environment

Within DHS, the Transportation Security Administration has used red teams to test airport security, and many observers say there is plenty of critical infrastructure that could stand to be subjected to red team tests — places such as chemical plants and rail transport systems.

Likewise, many businesses have long hired companies to do red-teaming of their own critical infrastructure. But some outside experts questioned the timing of the IAIP red team proposal, suggesting that DHS, and in particular IAIP, lacks the capacity to conduct red team operations on critical infrastructure effectively at this point.

"In theory, I think what they're proposing is great," said Bogdan Dzakovic, a former FAA red team leader. "But it's not going to work."

Dzakovic said the vulnerability of some critical infrastructure is now so patently obvious that "morons" could figure it out — as the Madrid rail bombing this month showed.

Likewise, he said, red teams are often neutered by top officials, who try to suppress their findings or limit their effectiveness by giving considerable advance warning to the security forces charged with repelling them.

What's more, the perception among intelligence and homeland security experts that IAIP has ceded its intelligence turf to the FBI and CIA led some to wonder how that directorate could credibly ascertain anything about terrorist motives or methods.

One House Democratic staffer, who asked to remain anonymous, asked, "If you haven't solved the intelligence question yet, what are you red-teaming?"

But the DHS official said that although "you always want more [intelligence] . . . part of the whole point of [red-teaming] is that as that [intelligence] circle continues to grow, you are always going to try and think beyond that circle."

And some critics of the Bush administration's homeland security efforts doubt the red teams would have enough leadership support.

"We should be rigorously testing to uncover our vulnerabilities in our nation's cyber security and critical infrastructure," said Rep. Martin Olav Sabo, D-Minn., the ranking member of the House Homeland Security Appropriations Subcommittee.

"With the administration and House Republicans doing all they can to shortchange homeland security, I wonder how seriously they will treat these important exercises," Sabo said.

Never Too Soon

But others applaud the initiative, even as they point out the challenges involved in composing and operating the teams.

"The bottom line is that it's never too early to know your weaknesses, then overcome them," said Rep. Dave Camp, R-Mich., chairman of the House Homeland Security's Infrastructure and Border Security Subcommittee.

Camp said the critical infrastructure red teams would be an "important tool in the war on terror." And Edward V. Badolato, who coordinated the Energy Department's nuclear emergency response and planning activities in the Reagan and first Bush administrations, said because al Qaeda has proved flexible in its methods, there is a need to try to figure out — via red team tests — what kinds of approaches they could take to launch successful attacks.

Badolato, a retired Marine Corps colonel who is now executive vice president for homeland security at The Shaw Group, calls IAIP undersecretary Gen. Frank Libutti a "good old Marine friend."

He said he has discussed the red team concept with other IAIP officials, and asserted that the agency's lack of intelligence-gathering capabilities won't ruin the red teams.

"If we accept that at this point IAIP is a consumer of intelligence rather than a generator of it, they will be provided for this particular red-teaming activity what I would judge to be adequate and competent information," Badolato said.

And he said even though DHS has adopted a non-regulatory approach to bolstering security in the private sector, the red teams could still net valuable information about how companies — many of which could not afford to run the tests on their own — respond to threats.

One key to IAIP's success, however, will be finding the right people to do the job. Badolato said the directorate should shun Ph.D. types in favor of people with military backgrounds. Some of the people expected to join the DHS red teams are counterterrorism experts who are already working in the department, the homeland security official said.

Different teams and experts will focus on specific components of the critical infrastructure, the official said.

'Nobody Gets Shot'

Dennis McBride, president of the Potomac Institute for Policy Studies, said the human element always makes red teams difficult to run.

The security forces subjected to red team operations, known as blue teams, often reject the red teams' conclusions, adding the need for "white teams" to referee the exercises.

And the entire process, McBride said, can be hampered if red team members aren't objective enough — or clever enough. A certain amount of cooperation between both sides is needed for all red teams, agreed Hank Chase, a retired Navy Civil Engineer Corps commander who led several critical infrastructure projects and now directs homeland security for ITS Corp.

"This is good stuff," he said, "as long as nobody gets shot."

Often that requires some kind of notification of when a red team might arrive, but there has to be some element of surprise, he said.

In at least one industry sector — ports — officials said they did not know enough about the red team proposal to comment authoritatively.

"We certainly know that everyone has beefed up security, that they've installed cameras and are implementing security plans, to the point that operational costs have increased dramatically," said Jay Grant, a lobbyist for the American Association of Port Authorities.

"I know some of the ports are expecting these. I would guess they would welcome them. The whole idea is to be ready if something happens."