

# Honeymoon over?

*Former CBP advisor Brian Goebel offers candid assessment of border security programs.*

By ERIC KULISCH

In the months after the Sept. 11, 2001 terrorist attacks, the U.S. government rapidly established the Transportation Security Administration to protect the passenger aviation sector, created several cargo and land border security programs, and helped generate an international maritime and port security code.

By March 2003, the Department of Homeland Security (DHS) opened its doors for the first time after the largest reorganization of the government in half a century.

The new department, preoccupied during the start-up phase with nuts-and-bolts organizational issues associated with melding 22 disparate agencies into a coordinated unit and later constrained by election year presidential politics, got the benefit of the public's doubt in making progress towards preventing another 9/11.

Now the honeymoon is over, counterterrorism experts and political observers say.

During the next four years, the Bush administration is likely to devote attention to strengthening those programs and launching new ones to address previously neglected vulnerabilities, spurred in part by renewed pressure from Congress.

The effort to keep terrorists and their weapons from entering the country without disrupting trade will likely focus on radiation detection, port security, private sector supply chain protection, cargo inspection programs in foreign ports, electronic container seals to detect intrusion, immigration reform and air cargo, according to Brian Goebel, an attorney in the Washington office of Gibson, Dunn & Crutcher, and as recently as eight months ago a senior policy advisor to Customs and Border Protection Commissioner Robert Bonner.

As one of Bonner's top lieutenants, Goebel helped play a key role in the U.S. Customs Service transition from the Treasury Department to DHS, integrating new immigration and agriculture inspection duties, creating the Container Security Initiative (CSI), the Customs-Trade Partnership Against Terrorism (C-TPAT) and the 24-hour advance notice requirement for ocean carrier manifests.



***“A lot of people haven’t been able to get into the C-TPAT program, but I think the real question is, when verifications really get going in earnest, will companies be kicked out?”***

**Brian Goebel**  
attorney,  
Gibson, Dunn & Crutcher

In a Nov. 9 speech to industry executives at a *Homeland Defense Journal* conference in Arlington, Va., Goebel offered his predictions on how the administration and Congress would tackle border and transportation security issues during the next four years.

**Radiation Detection.** Developing systems to identify nuclear material illegally entering the country will receive a lot of attention this year after Sen. John Kerry and President Bush stated during the

presidential debates that nuclear weapon smuggling is the greatest threat facing the United States, squarely framing the issue as a high priority in the public consciousness, Goebel said.

The most recent manifestation of the problem was the September raid by South African police of a factory outside Johannesburg, where elements of a two-story steel processing system for enriching uranium were found packed in 11 freight containers for shipment to Libya, according to the Nov. 28 *Los Angeles Times*.

The discovery is another piece of the extensive black market network set up by Pakistani scientist Abdul Qadeer Khan to sell nuclear technology to Muslim nations. Khan, the father of Pakistan's nuclear program, was shut down (but received a pardon by the government) after Italian authorities working on a tip from U.S. intelligence intercepted a freighter bound for Libya in October 2003, and seized wooden containers with centrifuge parts from a factory in Malaysia that served the Khan network.

“We don’t have our most sophisticated radiation detection systems at our ports of entry despite this vulnerability, so expect a concerted effort to get this equipment in place very, very quickly,” Goebel said.

CBP said it has installed more than 300 drive-by radiation portal monitors so far. These machines, which act like giant Geiger counters, are extremely sensitive, and can pick up small doses of radiation as trucks or cars pass through a checkpoint. But after 9/11, front-line inspectors had to rely on less accurate, short-range pocket-size radiation “pagers” worn by inspectors better suited for inspecting travelers than huge containers. At the time, the U.S. government was only using the technology along the borders of former Soviet republics under a cooperative threat reduction program to prevent smuggling of nuclear material. By September 2003, 60 of the large-scale detection arrays were in place in the United States, primarily at land border crossings. The systems are now being installed at seaports.

Congress appropriated \$50 million in fiscal 2005 for radiation portal monitors.

Goebel said the agency probably would get more money to complete deployment of the radiation detectors in supplemental legislation expected to be introduced early this year to support ongoing efforts in Iraq or, at the latest, in the 2006 appropriations cycle.

**Port Security.** The nuke-in-a-box threat also became a common refrain of the Kerry campaign. The Democratic contender repeatedly stated that the United States was vulnerable to attacks from nuclear weapons

## LOGISTICS

smuggled into the country because 95 percent of the containers entering through ports were not inspected. CBP officials argue that because the 24-hour rule and other advance manifest requirements for all shipments enable them to use automated database analysis to identify and sort out suspicious cargo for targeted exams prior to arrival.

Some security experts and industry officials who favor CBP's risk management approach, however, say the targeting system is still flawed because the manifest data is not detailed enough and is passed along to CBP by a third-party—the carrier. But the attacks by Kerry and other Democrats focused on the perceived need for more physical inspections of cargo—a scenario industry officials universally decry would lead to huge delays and shipping costs—rather than ways to fix this information gap.

Last summer, CBP said it was working with several importers to test ways to share sales, production and transportation information that is commercially available far before a shipment reaches the last port of departure for the United States.

DHS will continue to refine its system by working with the private sector to identify the best technology to support the information processing work that lies behind the exam process, Goebel said. At the same time, there will be heightened emphasis within the executive branch on getting more useful information from the intelligence community to support the targeting efforts, he said.

**C-TPAT.** A fundamental debate is going on within DHS and the trade community about the future of the C-TPAT and whether it should remain a voluntary partnership with industry or turn into a regulated program that sweeps all importers under its umbrella to increase the security of the supply chain.

C-TPAT was designed as a way to use private sector leverage to get foreign shippers, over which U.S. authorities do not have jurisdiction, to tighten up their security processes.

Customs has accepted more than 7,100 companies into the program, including importers, forwarders, brokers, carriers, terminal operators and ports, and some Mexican manufacturers. In exchange for assessing their security vulnerabilities, following guidelines on how to improve any gaps and making similar demands on their foreign suppliers and transportation providers, importers are promised fewer inspections and delays by CBP. But a manpower shortage has slowed the agency's effort to make field visits and validate that companies are following through on promised improvements. So far, only about 400 companies



**CBP officers check an individual's luggage.** (Photo credit: James R. Tourtellotte)

have been verified as full members eligible for all C-TPAT benefits.

C-TPAT is under pressure from some lawmakers and others who are inherently suspicious of government-private partnerships and feel the program does not have enough teeth. Goebel said it remains an open question whether C-TPAT as it is formulated will survive, despite the support of many in the import business who believe it provides adequate incentives to improve security. Part of the problem has to do with “free riders” in the trade community who have signed up for C-TPAT but are not doing much to actually improve their supply chain security because they assume there is slim chance CBP will check on them.

CBP is expected to soon announce more rigorous criteria for companies who want to participate in C-TPAT, but many in the trade community worry that if the rules are too strict and costly companies may opt not to join the program.

The larger public policy debate will likely hinge on whether CBP and the trade can actually demonstrate a verifiable increase in supply chain security, particularly at the point of stuffing, according to Goebel.

“The reality is we are not there yet. We have a lot of anecdotal information about increased supply chain security” but the vetting process is still in its earliest stages,” Goebel said.

CBP's Advisory Committee on Commercial Operations, comprised of industry officials, repeatedly urged the agency in 2004 to share empirical data on the success of enforcement activities as a way to convince companies of C-TPAT's worth.

“I think a lingering question is whether that (validation) is a function the government will ever be able to do on its own, or whether you'll have to bring in third parties,

private sector specialists, to be involved in that process,” Goebel said.

The other key question facing CBP is whether the program has enough teeth to ensure compliance.

“Until you kick people out how can (you) really have confidence that the C-TPAT members are doing what they pledged to do, and that the program is really going to increase our security?” Goebel asked.

“A lot of people haven't been able to get into the C-TPAT program, but I think the real question is, when verifications really get going in earnest, will companies be kicked out? People on the Hill and in the policy community who think the program is not stringent enough will not be satisfied until they see some people booted out of the program,” he said.

Unless CBP can show progress on both counts, the administration and Congress will consider replacing C-TPAT with a mandatory, regulated program, he predicted.

**CSI.** CBP has credited CSI, launched in early 2002, with giving it an over-the-horizon capability to stop high-risk containers before they depart for U.S. shores. Through bilateral agreements with other nations, the United States is stationing inspectors at foreign ports to identify suspicious containers flagged by the agency's automated targeting system. Under the reciprocal program, national customs authorities conduct the actual cargo exams using high-tech x-ray equipment to search for contraband and other materials that do not match the contents in the manifest.

So far CBP has CSI officers in 32 ports, which account for about 80 percent of U.S. import volumes. The border security agency plans to continue expanding to more ports in 2005, including ones in the

Middle East, Africa, and, for the first time, South America.

But relatively unrecognized is the fact that CBP officers are only inspecting a tiny fraction of available containers, in part due to the small size of the CSI teams. Some in Congress want proof the program is working as advertised.

Goebel said pressure will mount on CBP to do more inspections in CSI seaports in the months ahead. One positive development that will act as a force multiplier is that the Canadian government is also planning to put customs officers in foreign seaports, including ones where U.S. personnel are not located, to ensure that containers that pose a threat can't get to the United States through Canada, he noted.

CBP will soon reach a crossroads when it will have to decide when to stop expanding the program to more ports, Goebel said. The first phase of the program focused on the top 20 container ports in terms of volume shipped to the United States, followed by a second phase targeting ports in high-risk areas of the world.

"At some point it is likely you will see diminishing marginal returns. Thirty seaports are clearly not enough, but there is no way we can go to 600," Goebel said.

"I'm not sure where you draw the line. I know you can't just build a Maginot Line. You can't protect 30 seaports and leave us exposed to hundreds of other ports," but covering 100 percent of containerized cargo ports is equally impractical, he added.

Goebel predicted that CBP will soon start to develop the criteria for deciding when to cap CSI.

At the same time, the administration has to find a way to expand the Department of Energy's Megaports Initiative, which loans radiation detection equipment to foreign governments to help scan cargo moving through hub seaports (October 2003 *American Shipper*, page 80), he said. So far, the CSI companion program has only installed detection equipment at the Dutch port of Rotterdam in September 2003 and the Vilnius Airport in Lithuania in 2004, in part because governments have declined to request assistance. In late November, the Energy Department said the government of Belgium had agreed to accept radiation detection equipment at the Port of Antwerp, and Goebel said he expected more countries to follow suit.

**Smart Box.** CBP Commissioner Bonner outlined his vision for a more tamper-evident, tamper-resistant ocean container in late 2003, but DHS officials acknowledge that commercial deployment of so-called "smart box" technology — which can provide status

## NIT League rejects C-TPAT revision

### WASHINGTON

The National Industrial Transportation League strongly criticized the revised security standards proposed in November by the U.S. Customs and Border Protection for importers participating in the Customs-Trade Partnership Against Terrorism (C-TPAT), saying the standards are "unrealistic, unworkable and vague."

The second-draft proposals maintain C-TPAT as a voluntary program, but are more direct than the current guidelines in spelling out security measures that importers and their non-U.S. suppliers are expected to take in exchange for reduced levels of inspection and eligibility for certain automated customs payment programs.

In a Dec. 3 letter to the Office of Field Operations, the Arlington, Va.-based NIT League said it has major concerns over the revised security standards for importers proposed by the agency, and that they may force importers to leave the voluntary program or deter them from joining it.

The NIT League urged CBP to continue to work with industry to modify the security standards, despite Customs' stated intention to introduce new standards as early as the end of this year.

Under the draft criteria, companies would be required to conduct a risk assessment of their supply chain and make any changes to plug security gaps.

The league told the agency it should define the criteria to be considered by importers in performing a security risk assessment, instead of leaving it to individual companies. "Otherwise, it is likely that importers will assess risk in vastly different ways which, in turn, will lead to the implementation of inconsistent and potentially conflicting security measures," the NIT League said. Without CBP's expertise, importers could make wrong assumptions about security that are not shared by CBP officers, the NIT League added.

The NIT League also questioned the standards' mandatory approach, saying they clash with the voluntary nature of the C-TPAT program and raise issues of liability for the companies concerned.

"There are significant concerns on the part of importers that by agreeing to adhere to the new standards they will become potentially liable to third parties, in the event of a future incident that causes personal injuries or property damage," the NIT League said. "It is the change to the more mandatory language that creates this potential liability. The fact that CBP may not intend to strictly enforce the C-TPAT standards does not reduce the liability that importers, arguably, may have to third parties, based on the importer's 'agreement' to implement the standards.

"In such a case, the liability exposure conceivably could be catastrophic for a company."

The NIT League said it is impractical to hold importers accountable for ensuring that foreign suppliers and service providers, over whom they have no control, adhere to C-TPAT standards and practices, including the requirement that business partners fill out a questionnaire documenting their security controls.

"CBP has wrongly assumed that most importers maintain sufficient leverage over their foreign manufacturers, suppliers and vendors, which will ensure that such entities will agree to respond to the questionnaires and to implement corrective security measures imposed by the U.S. importer," the freight transportation trade group said.

On container security, the NIT League agreed importers must require that procedures exist at the time of container stuffing for the inspection of the container and for the affixing of a high security seal when the container has been loaded. However, the shipper group said it is "not reasonable to impose mandatory requirements on importers for activities that occur overseas at the point of container stuffing, sealing, or storage, since the importer will not be able to effectively enforce such requirements" on third parties.

"Although improvements were made to the second draft, there are still significant problems that need to be addressed by CBP," the NIT League concluded in its letter, urging the agency not to adopt the proposed standards.

reports on cargo throughout the journey or at critical transshipment points — is at least three years away. High false alarm rates are one of the main sticking points they cite.

Goebel said a smart container device won't be required on shipping containers until the government can define its purpose and complicated operational parameters

(October *American Shipper*, page 18). Questions that still must be answered include:

- Does it need to have satellite tracking and communications to enable 24/7 monitoring, even though the container spends most of its time on a vessel whose location is known?
- What types and number of sensors should be installed on a container to detect changes in light, temperature, air pressure, radiation, open doors and other variables, and what party should be notified of a potential breach?
- What technology can accomplish this in a cheap and reliable manner?
- Can the technology be recycled for repeated shipments?
- Who can communicate with the technology? CBP, the trade, foreign customs authorities?

Acting as a potential brake on the whole concept of instrumented containers, is the likelihood that one of the millions of containers that circulate around the world will fall into the hands of terrorists, drug traffickers or arms merchants who could exploit the technology to develop countermeasures, Goebel cautioned.

“Do we want some of our most sensitive and sophisticated technology out there for the picking?” he said. “That is something that needs to be thought through before we decide to put sophisticated chemical, biological and radiological detection equipment in a shipping container.”

**Air Travel.** The U.S. government “still essentially has done nothing to stop the next Richard Reeve (the Shoe Bomber) from getting on an airplane” to the United States, Goebel said, even though in December 2003, the Transportation Security Administration had to delay and cancel flights from Britain and France because security personnel, operating on intelligence about terrorist travelers, couldn’t screen passengers against terrorist watch lists before the planes took off. In October, the musician formerly known as Cat Stevens, a convert to Islam who is on a terrorist watch, was discovered on a United flight from Europe while the plane was in the air, forcing the plane to be grounded in Maine.

The problem is that the government has no equivalent to CSI and the 24-hour rule for passengers, Goebel noted. Bonner launched

the Immigration Security Initiative as a passenger version of CSI in early 2004, but lacks the resources to implement the program. Under ISI, the agency will place small teams of officers at major international airports to work with airlines and host governments to inspect high-risk passengers and make sure they have valid entry documents before they board an aircraft. So far, the United States only has an agreement in place with Poland to station officers at Warsaw International Airport. The 2005 Customs appropriation includes about \$1 million for the program, compared with \$125 million for CSI.

Goebel said he expects the government to crank up efforts to stop potential terrorists from boarding planes overseas because it received some attention in the Sept. 11 Commission report and is dealt with in the recent intelligence reform bill.

DHS will begin rolling out ISI teams to foreign airports sooner rather than later, he said. He also predicted a major rulemaking from DHS, or legislation, to get CBP officers passenger manifest and name record data they need before boarding, much like CBP used the 24-hour advance manifest rule to get information on cargo before it was loaded on a vessel, rather than before arrival.

“This is something that can be done in

a way that doesn’t disrupt international air travel, and I’d like to see it happen soon,” Goebel said.

Such a rule would provide a major benefit to airlines by relieving them of the duty of administering the “no-fly” list and cost savings if they make a mistake. Airlines pay a \$10,000 fine for transporting an inadmissible individual, plus have to make a seat available to return the traveler to the origin airport.

**Immigration Policy.** U.S. policy has to decrease the number of people seeking to illegally cross the border and simultaneously apprehend everyone that does, Goebel said, noting the reported presence of terrorist cells in Canada, Mexico and South America.

Goebel said he expects several policy initiatives designed to substantially increase funding for the Border Patrol, raise the ceiling on lawful immigrants and create a guest worker program. The government will have to decide to what degree to link foreign aid to Mexico to that country’s ability to control its southern border and the flow of people crossing its northern border into the United States.

**Air Cargo.** Tucked in the fiscal 2005 DHS appropriations bill is a rider that directs the

department and TSA to develop systems for screening cargo on passenger planes, take interim steps to improve the “known shipper” program and triple the inspection rate for cargo on passenger planes.

In November, the TSA issued long-awaited proposals to strengthen air cargo security that address some of these provisions, including enhancing the known shipper program by tightening requirements on freight forwarders to properly screen allowable shipments.

The mandate from Congress falls short of calls by some lawmakers to inspect 100 percent of cargo on passenger planes, but shows increasing impatience by lawmakers with current efforts.

“This provision could be the first step down the slippery slope to a 100 percent inspection rate,” Goebel said.

The extent to which airlines and shippers are impacted may depend on whether TSA defines inspections as physical exams, or simply collection and analysis of shipping data for red flags, similar to CBP’s targeted inspection approach.

Either way will impose addi-

## Catching WMDs

### WASHINGTON

The National Nuclear Security Administration said in October it is expanding its efforts to train border guards and customs officials in other countries to halt illegal smuggling of nuclear, chemical and biological weapons equipment and technology.

The NNSA, a U.S. Department of Energy agency, said it has designed a new Commodity Identification Training curriculum to educate and train customs inspectors and border guards in detection and interdiction techniques.

Eleven countries, including Lithuania, Georgia, Turkey, Thailand and Ukraine are participating in the training courses. Latvia is the most recent country to join the program and has formally added the weapons-of-mass destruction (WMD) training to the curriculum for its customs personnel, with plans to provide it to on-duty customs personnel on a rotating basis.

“Our goal is to help partner countries incorporate WMD training programs for customs inspectors, investigators, border guards and other key personnel,” NNSA Administrator Linton Brooks said in a statement.

The program is part of the U.S. government’s strategy to reduce proliferation of dangerous materials and weapons, which includes a multilateral initiative to stop suspect ships on the high seas, as well as securing, removing and disposing of uranium and other nuclear fuels in parts of the world where stringent controls are not in place. The NNSA also manages the Megaports Initiative through which the department loans high-tech equipment that detects radiation in large shipping containers.

tional costs on airlines. CBP has a system in place, the Automated Air Manifest System, to capture prefiled electronic shipping data before the plane takes off. Planes with high-risk shipments can be turned back. But no similar system exists for domestic flights. It is unclear whether the legislation demands this type of information system, the former CBP official said.

Fixing the known shipper program, which allows companies that meet certain security requirements to ship goods on passenger aircraft, has proved elusive for TSA so far. One unfulfilled goal has been to run shippers against a terrorist watch list, in part because the government has not been able to consolidate lists of suspects from various agencies into a master list. Goebel noted that conducting such matches is problematic without some automated system for sharing commercial cargo data with TSA.

Even with such a system, TSA would need to figure out a protocol on how to respond if there is a match. For instance, would a shipper be subject to 100 percent inspections, be prohibited from shipping via passenger airlines, or banned altogether from shipping by air?

"These are issues that have plagued the TSA in the no-fly list area and are going to be raised in the known shipper area as well," Goebel said.

The language of the bill — "until such (screening) technology is procured and installed" DHS "shall take all possible actions to enhance the known shipper program" — also raises questions about the future of the program. Congress appears to be leaving the door open to canceling the program at some point, especially if it goes to a 100 percent inspection regime for cargo on passenger aircraft. Goebel and his firm are advising clients not to make substantial investments to improve their known shipper processes until the government clarifies its intentions.

The legislation is also ambiguous about whether the directed inspection rates apply to domestic or international air cargo.

A determination that the law applies to international shipments too will create bureaucratic tension between CBP and TSA over who has primacy for international air cargo, Goebel predicted. TSA said in its *Federal Register* notice that the proposed air cargo rules complement CBP's programs. However, if TSA programs are not well reconciled with CBP's existing manifest prefilling system then the industry could face additional requirements and costs, such as connecting to a separate computer system, to submit cargo data.

Expanding security requirements to in-

ternational flights also creates legal issues because the government would have to figure out how to implement such a system in accordance with International Civil Aviation Organization rules. And it raises the possibility of CSI and C-TPAT programs for air cargo, Goebel said.

Since the formation of DHS, some industry observers have wondered why TSA is struggling to devise air cargo security programs from scratch, instead of borrowing and applying the CBP model of risk management and targeted inspections that is already in place. Industry officials always worried about the TSA being the lead agency for dealing with cargo security, but the DHS border and transportation security bureau has since taken over that role.

An important policy question before DHS, Goebel said, is whether to adopt an equivalent C-TPAT/CSI program for air cargo in which shippers take responsibility for securing their supply chains, and the government gets commercial shipping data about cargo before it gets put on a plane. In the fiscal 2004 DHS appropriations bill, Congress directed TSA to consider testing the expansion of C-TPAT to the domestic air cargo supply chain.

"It may be a worthy goal, but it will take great cooperation from the private sector in order to make it happen given the way carriers move international air cargo in the United States," Goebel said.

How these issues are addressed "could determine whether it would be economically feasible for air passenger carriers to carry overseas cargo" anymore, he added.

**DHS Structure.** After almost two years in existence, DHS has some critical organizational issues that need to be cleared up, according to Goebel.

A big question that needs to be addressed in order for the department to function smoothly in the years ahead is whether the Science and Technology directorate "is set up as an operational office that exerts some degree of control over technology choices and operation of technology by underlying agencies, or is it just a an R&D shop for basic research and grant administration designed to put in place the next Manhattan Project for nuclear, chemical and biological detection" Goebel said.

The lines between the TSA and the Information Analysis and Infrastructure Protection directorate are also fuzzy, according to the Gibson, Dunn attorney. It is not clear who has the lead when it comes to protecting domestic transportation systems like rail, he said.

As air cargo policy is further developed, DHS must decide what role, if any, TSA

should play in the international arena given CBP's statutory authority in that arena, according to Goebel.

The most controversial organizational change suggested by Goebel goes to the heart of DHS's management structure. The Department of Justice, for example, has a flat, lean organizational structure in which the FBI and other agencies report directly to the deputy attorney general. DHS officials, guided in part by the Homeland Security law that authorized the department's creation, created the Border and Transportation Security (BTS) directorate through which CBP, TSA, Immigration and Customs Enforcement and other agencies report. At the same time, the U.S. Coast Guard reports directly to the secretary outside the BTS chain of command.

"This is a fairly curious organizational model to say the least," said Goebel, who interacted closely with BTS during his Customs tenure. Other sources have noted that CBP is chaffing under what it perceives as micromanagement by the BTS directorate.

DHS policymakers are considering replicating that extra layer of management for agency offices in the field. For the last 20 months, the trade community has nervously waited as the department develops plans for a regional management structure designed to let sector chiefs coordinate efforts and information sharing between multiple agencies, liaison with local government and manage contingency plans for disaster response.

The import/export community has vigorously fought such a regional proposal out of trepidation that different regional directors will dilute direct communication to and from ports of entry and undermine uniform Customs enforcement, leading to port shopping by shippers for better treatment. The regional format has languished since February 2004, when DHS officials said they were on the verge of announcing their plan.

Goebel said the department apparently went back to the drawing board and could unveil its regional proposal soon.

He said the regional structure makes sense on many levels, but agreed that it could break the direct chain of command between the ports and agency heads, leading to confusion on the ground for Customs personnel and importers alike. Goebel also concurred with trade groups that an extra layer of senior management has the potential to undercut uniform policy implementation.

"You don't want Newark to have a 57 percent cargo inspection rate and L.A.-Long Beach to have 0.1 percent, he said. "It's not a regional terrorist threat, it's national." ■