For its part, the port authority said American Stevedoring overbooked the limited space it had available at Pier 9. In February, Steve Coleman, a port authority spokesman, reiterated for *American Shipper* comments he had made earlier: "in the past, we've been willing to help them out. But we're not willing to provide the additional space so that it can be mismanaged again."

The Red Hook piers are owned by New York City and leased by the port authority, from which American Stevedoring subleases its warehousing space.

The port authority told *American Shipper* that while it wasn't owed rent by American Stevedoring, a subsidiary of that company, American Warehousing, was in arrears for rent.

An American Stevedoring spokesman said the port authority had doubled its warehousing rent and then refused payments that a court had ordered the port authority to accept. Denying any mismanagement on its part, American Stevedoring said the port authority wanted to turn as much business as possible away from the Red Hook piers.

The port authority confirmed it will not renew American Stevedoring's lease when it expires in 2007.

At first, this episode seemed destined to be an internal harbor squabble — until word got out, with a story appearing in *The New York Times* about the plight of the *DS Freeway*.

The longer the impasse lasted, the wider the circles of incredulity spread. U.S. Rep. Jerrold L. Nadler, whose district includes Red Hook, agreed with the port authority that the South Brooklyn Marine Terminal in Sunset Park would be "a better place for a port — but you don't close Red Hook down until you have another place ready to go."

As for the *DS Freeway,* it took seven days for space finally to be found on Pier 9 for the ship's cocoa. The vessel's owner, Sabrina Shipping, held out because it wanted to use the experienced cocoa handlers available at Red Hook.

Perhaps the port authority should commission a sequel to Richard Wagner's opera, *The Flying Dutchman.* In this updated version, a ghostly vessel loaded with bulk cargo destined for Red Hook could call ceaselessly, without avail, at piers in the other boroughs of New York and along the New Jersey waterfront — for seven days, until a warehouse could be found and the port authority's self-defeating curse lifted.

From any angle, it's a hell of way to run a harbor. *(Robert Mottley)*

DHS caught in its own trap

The Department of Homeland Security, in its wisdom, has decided that smart containers are smart only if their doors are smart — it will be able to detect the opening of the doors.

Industry has decided that radio frequency identification is the preferred technology to detect and transmit the door breach. Unfortunately, DHS and the major industry players do not understand the irony and risk posed by both DHS container security criteria and industry's dedication to RFID applications in creating smart containers. Although this danger could not have been their intent, they have, nonetheless, created the formula for and means of detonating explosive devices in our ports.

Here's what is known and can be demonstrated factually.

Fact No. 1: In the latest Request for Information, an information-gathering and planning vehicle used by DHS in support of Customs and Border Protection, Johns Hopkins University's Applied Physics Laboratory (under contract with DHS) sent a letter dated Nov. 8 to potential vendors. The letter stated in part, "The purpose of this request is to gather information to identify and evaluate available state-of-the-art container and trailer tracking devices suitable for in-bond shipments." That statement, alone, poses two serious questions. What does DHS believe is "state-of-the-art," and why has it taken this long after 9/11 for DHS to realize CBP had little or no knowledge of or control over containers coming into the United States and moving throughout the U.S. under bond.

The level of "state-of-the-art" for DHS is the following:

1. *Sensing*
   a. *The container and trailer security device must be able to electronically detect closing and opening of either door of the container/trailer. Monitoring the door status must be continuous from time of arming to disarming by authorized personnel.*

Fact No. 2: In April 2005 a North Carolina firm demonstrated to national and foreign attendees, including the news media and the Defense Department, the capacity and ability to breach a container, and insert contents into the container without ever opening the doors. Additionally, that same firm through the cooperation of EADS in Bremen, Germany, repeated successfully on multiple occasions that same demonstration.

Fact No. 3: Under a contract from the U.S. Energy Department, that same North Carolina firm in 2004 demonstrated in Laredo, Texas, the nation's largest southern border port-of-entry, the capacity and ability to insert clandestinely RFID antennas not detectable from outside the container which would trigger an electronic signal *within* a locked container when energized by an RFID transceiver located *outside* the container.

Fact No. 4: In June 2004 the Federal Communications Commission issued a final rule authorizing the use of 433 MHz for commercial shipping containers. Since each nation or region approves and utilizes different frequencies and communication

protocols, frequency identification is easily obtained through published government documents. Even wattage is specified. In the United States, 433 MHz used in commercial shipping containers must use less than 100 milliwatts, necessitating the need for cutting in an antenna into the container (Fact No. 3). Although the frequency is low enough to penetrate the steel of the container, its limited wattage requires the use of an antenna.

Fact No. 5: The large-firm entrants into the smart container market have been identified as IBM-Maersk, GE-NYK, Siemens-GE, Motorola and SAVI. It has been reported that each is dedicated to and has developed smart container devices employing RFID technology. This technology will require the use of an RFID transceiver at certain foreign and U.S. ports. In U.S. ports these transceivers will interrogate inbound containers equipped with their devices by using 433 MHz, the only U.S.-approved frequency for the commercial shipping container market (Fact No. 4). Because they are published, the identification of U.S.-approved frequencies like 433 MHz used in the commercial shipping containers is available to any terrorist.

Fact No. 6: The combination of these factors provides the model and means of detonating explosive devices surreptitiously placed into locked RFID-equipped containers which when interrogated, transmit a "breach" or "non-breach" signal at destination in a U.S. seaport or in the case of motor carriage, at land port-of-entry.

Assume a container departs a foreign factory en route to a foreign port for sea carriage to the United States. En route the container is breached without opening the doors (Fact No. 2) and shielded nuclear waste along with an explosive device are placed into the container. An RFID antenna is cut into the wall of the container by a terrorist unseen from the outside, a 15-minute process (Fact No. 3). The container continues its journey into the foreign seaport for lading into a U.S.-bound vessel. The dirty bomb device can then be automatically armed by the interrogation signal of an RFID transceiver placed at the foreign port. The transceiver signal rides on an RFID frequency approved by the government of the foreign nation from which the container will be carried to the United States (Fact No. 4). However, given the additional differences of communication protocols among different regions of the world, it would even be simpler to insert an explosive device already armed. Even simpler would be to breach the container, place the explosive device and install a door switch to detonate the bomb when the doors are opened.

The container is subsequently loaded into the vessel which sails to the United States. Upon its discharge from the vessel, the locked container is interrogated in the U.S. seaport, responds with "safe condition" and then explodes. It explodes because the bomb was set to detonate upon receiving the mandated 433 MHz signal from the RFID transceiver, properly approved, installed, and used by those companies depending on RFID for container security.

This scenario can happen because we let it. DHS policies specifically are responsible for this scenario. Additionally, industries' concern over costs, the degree of influence by industry lobbyists, and the lack of congressional oversight of a department with questionable experience and knowledge in container security all seem to share the blame.

What can we learn? First, door-only security is not only inadequate, but also dangerous. It represents a lack of either knowledge or sophistication, or both. It may even represent the acquiescence of DHS to industry lobbyists representing companies who have committed, perhaps foolishly, many dollars to RFID door-only applications. We must switch to end-to-end security applications that help monitor the security of the container at stuffing, which detect breaches through any part of the container and transmit the breach notification via satellite in real time, not delayed RFID time. Second, RFID for many other reasons should not be the preferred technology for global container security. Third, we must realize that essential characteristics of radio signals can serve as the very means of detonating explosives placed in the container. Finally, the current leadership and the quality of decision-making of DHS personnel assigned to container security suggest a need for serious review and re-evaluation.

James Giermanski
director, Center for Global Commerce,
Belmont Abbey College
Belmont, N.C.

Insurance coverage for port politics

Port management is inevitably a balancing act between politics and operations, whether that means dealing with two governors in New York and New Jersey or city councils in Los Angeles and Long Beach.

At Port Everglades in South Florida, local politicians tried to cover both bases by naming a veteran from within the local county government as its new port director. Phillip Allen, Broward County's chief financial officer since 1986, was described by officials ranging from the county commissioners to Allen himself as a means of stabilizing management at the port.

Allen was selected by interim county administrator Bertha Henry and endorsed by a vote of the county commissioners Feb. 7 after Henry told the commissioners Allen would bring in a veteran from the ports industry as a deputy director.

Previous directors Kenneth Krauter, who came from the Port of Jacksonville, and Paul DeMariano, who came from the Port of Philadelphia and Camden, were port professionals who publicly clashed with now-retired county administrator Roger Desjarlais. Local officials apparently hoped to avoid a third clash with an industry professional by making the new director a person who can effectively act as a pilot in the local political waters, with an industry professional helping to guide the vessel in the open seas.

Allen is unusually well-based for someone not directly from the ports industry. He had served as interim port director since last June, and was also named interim director in 2000 and 2001, between the tenures of DeMariano and Krauter. He certainly experienced baptism under fire, having been in charge of day-to-day operations at the port in the immediate aftermath of Sept. 11, 2001, and during 2005's hurricanes Katrina and Wilma, which both passed directly over Port Everglades. *(Jim Dow)*

Correction

February's issue should have said Deep R. Parekh is with Equus LLC. His e-mail address is deep.parekh@equusllc.com. The source for two charts within Parekh's story (page 28) was Equus Research 2005.