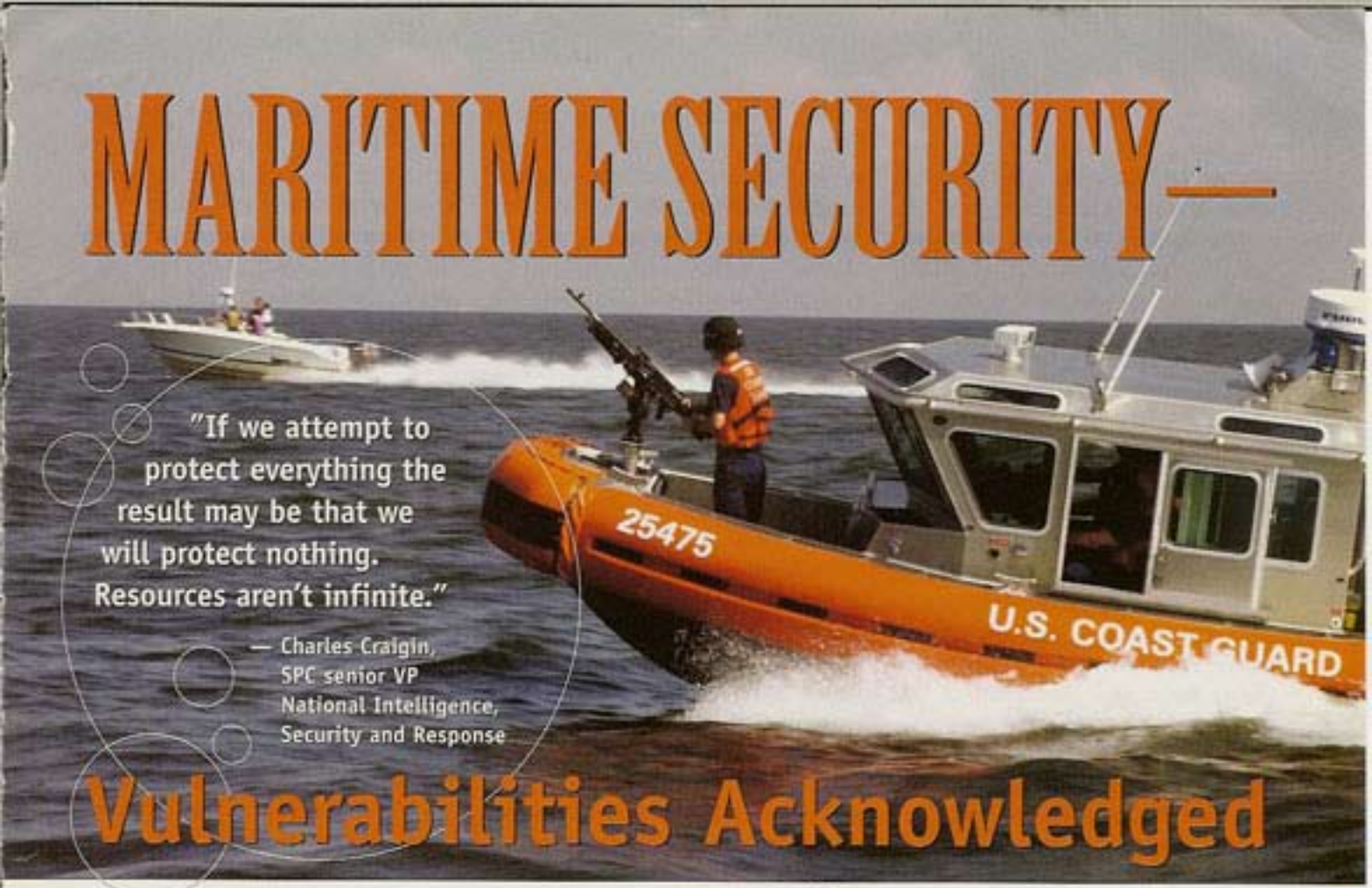
MARITIME SECURITY—



"If we attempt to protect everything the result may be that we will protect nothing. Resources aren't infinite."

— Charles Craigin, SPC senior VP National Intelligence, Security and Response

Vulnerabilities Acknowledged

By David C. Walsh

USCG

U.S. PORT SECURITY EXPERTS SHED LIGHT ON THEIR ORGANIZATIONS, DETAILING THE INTRICATE WAYS THEY INTERACT and, more importantly, how they intersect with the multi-directorate Department of Homeland Security (DHS). The industry veterans spoke at the Homeland Defense Training Conference®: Transportation Security Executive Briefings on Port & Maritime Security in September.

At the three-day conference there was talk of advanced container-screening and sealing technology; surface transportation nodes; civilian contractor vetting; certifying off-duty police officers to work at ports and terminals; and strengthened government/business links. But most of all, there was discussion about the enormity of trying to guarantee port security three years after the terrorist attacks of Sept. 11, 2001.

Ninety-five percent of the world's goods — worth some $500 billion — move via maritime transportation yearly to several hundred U.S. ports, in about five million containers. Of the 15,000 containers arriving daily, the total cargo visually inspected is 5.7 percent. Are seas and docking points the next target-rich environment?

Charles L. Cragin, senior vice president of national intelligence, security and response at System Planning Corp. (SPC) and chair of the event, reminded the crowd of the degree to which the nation depends on seaborne commerce. "The closure of U.S. ports for more than two weeks would begin to destroy the [American] economy and seriously threaten global economic disaster."

Despite an estimated $7 billion in costs over the next decade to port officials and ship lines, many operating on small margins, Congress authorized just $500 million in port security grants under maritime edicts, such as the Maritime Transportation Security Act of 2002 (MTSA). Craigin noted that security gaps linger: 110,000 fishing vessels are not required to comply with the MTSA, nor are small craft such as the "suicide dinghy" that killed 17 sailors on the U.S.S. Cole in 2000.

However, he noted, "If we attempt to protect everything the result may be that we will protect nothing. Resources aren't infinite."

BROADENED RESPONSIBILITIES

Brig. Gen. Mark Scheid, operations director, Surface Deployment and Distribution Command (SDDC) at Fort Eustis, Va., noted some changes in his global organization, which is part of the Department of Defense's Transportation Command. He said since Sept. 11, 2001, SDDC has been responsible for command and control — from pickup stateside to delivery abroad — even contracting for delivery trucks and the like in Iraq, Kuwait and elsewhere. The job is much

broader than portal-to-portal, Sheid said, noting that it now includes inventory control, video and other technical means of ensuring cargo integrity

After cargo is in-country, Sheid said, radio frequency identification (RFID) tags are used to track military materiel. Monitoring techniques are improving, but, he added, "We're still a little bit short on satellite tracking." Global Positioning Systems (GPSs) are useful but don't penetrate below decks

The degree of SDDC's logistical coordination with other U.S. commands — Central (CENTCOM), Northern (NORTHCOM) and Transportation (TRANSCOM) — is staggering. It must be, Sheid noted, involving stupefying amounts of ordnance and other volatile shipments plying the oceans in support of the warfighter.

Here, he noted, SDDC provides very little of its own security, relying instead on "layers and layers of force protection."

DHS, the Coast Guard, Naval Criminal Investigative Service, Army military intelligence, CIA, FBI, law enforcement authorities and other government and civilian entities combine to secure ports used by military and commercial shippers. At lower levels, Sheid said, federal, state and city officials join with civilian contractors, local truck drivers and civilians to secure ports.

Best practices start with each military unit being responsible for initial packing and inspection of its goods, Sheid emphasized. More broadly, SDDC gets national agency intelligence daily about suspect activities across the globe.

LIVING HOMELAND SECURITY EVERY DAY

Lt. Cmdr. Lee Boone, chief of the compliance department, U.S. Coast Guard, Baltimore, said his service "lives homeland security every day," in intimate contact with DHS and many of its chief constituents: Transportation Security Administration (TSA), U.S. Customs and Border Protection, Immigration, FBI, first responders — essentially the same interlocking panoply of which Sheid spoke.

"We rely heavily on partnerships to carry out our mission since we're a small service," said Boone. He outlined vessel-boarding procedures, and the many complex data-sharing links that tie agencies together in multiple ways. Adding to the complexities, the 12-year Coast Guard officer stressed, the sea service's tasks must "balance security with [civil] liberties"— both at his Baltimore district and other busy American ports.

Much of Boone's work involves "increasing maritime awareness—awareness of assets, vulnerabilities, special hazards in port, locations of facilities and vessels."

These initiatives, he said, are all aimed at "intercepting threats well before they reach our shores."

Recent Coast Guard accomplishments, Boone said, include meeting the "red-letter day" of July 1, 2004, when the International Ship and Port Facility Security Code (ISPFS) went into force. Announced in 2002, the code required the United States and other participating countries to deploy inspectors to one another's ports, ensuring compliance with its security mandates.

On this end, every foreign ship making its first trip is boarded, and ships of nations that haven't signed on to ISPFS are tracked. The Coast Guard could deny entry to vessels from noncompliant countries, as well as intrusively inspect them at sea and take other measures, Boone explained. The ISPFS agreement falls under the United Nations International Maritime Organization.

The Container Security Imitative (CSI) is another program Boone cited as highly useful in helping the Coast Guard secure and speed maritime commerce. Although a product of the Bureau of Customs and Border Protection (CBP), the two agencies work closely on it. CSI includes 96-hour advanced notice of arrival for all 300-ton-and-greater incoming vessels from abroad. Each, Boone pointed out, must give ports-of-call, state flag, cargo manifests and lots of other data.

Undertaken in coordination with about two dozen nations to date, CSI, similar to ISPFS, involves "exchanges." U.S. officials are stationed abroad to work with foreign counterparts and vice versa. The aim is to secure the supply chain before cargoes are loaded.

CIS outlines punitive measures if goods turn out to be suspect. It also covers, to a degree, certification of security personnel. As with similar initiatives, CIS permits berthing denials, interceptions by Coast Guard cutters, and other actions. Such interlaced, proactive measures are vital, specialists said, because in many countries port security is slapdash.

The Coast Guard must help implement mandates under CIS, MTSA and ISPFS for vessel I.D. and port safety/security compliance. "You might be thinking this is a huge burden for the maritime industry — and you're right: $7 to 10 billion over the next 10 years," Boone said, adding that the private sector must contend with "huge amounts of policy and regulations" to pass multiple kinds of port security assessments — all of them a costly and time-consuming result of 9/11.

MTSA IMPLEMENTATION

Reserve Navy Lt. Cdr. Kevin Krick, senior adviser in maritime policy to the U.S. Maritime Administration (MARAD), helped draft the MTSA. His organization works most closely with the Coast Guard and is also active in the MTSA's vessel identification requirements.

MARAD also is instrumental in certification courses for various levels and kinds of maritime security personnel. Individual graduates coordinate with a ship's security officer, local law enforcement and military police, among others. Given the disparate organizations seeking guidance and certification, a large part of MARAD's mission was to "bring these people up to speed" with proper ship and maritime industry safeguard procedures, Krick said.

While highly professional in their own realms, they typically aren't steeped in requirements in "this specific maritime environment." Seeing this, and hearing industry and mariners' calls for standardization, "We created a MARAD/Coast Guard/MTSA109 Committee," said Krick.

broader than portal-to-portal, Sheid said, noting that it now includes inventory control, video and other technical means of ensuring cargo integrity

After cargo is in-country, Sheid said, radio frequency identification (RFID) tags are used to track military materiel. Monitoring techniques are improving, but, he added, "We're still a little bit short on satellite tracking." Global Positioning Systems (GPSs) are useful but don't penetrate below decks

The degree of SDDC's logistical coordination with other U.S. commands — Central (CENTCOM), Northern (NORTHCOM) and Transportation (TRANSCOM) — is staggering. It must be, Sheid noted, involving stupefying amounts of ordnance and other volatile shipments plying the oceans in support of the warfighter.

Here, he noted, SDDC provides very little of its own security, relying instead on "layers and layers of force protection."

DHS, the Coast Guard, Naval Criminal Investigative Service, Army military intelligence, CIA, FBI, law enforcement authorities and other government and civilian entities combine to secure ports used by military and commercial shippers. At lower levels, Sheid said, federal, state and city officials join with civilian contractors, local truck drivers and civilians to secure ports.

Best practices start with each military unit being responsible for initial packing and inspection of its goods, Sheid emphasized. More broadly, SDDC gets national agency intelligence daily about suspect activities across the globe.

LIVING HOMELAND SECURITY EVERY DAY

Lt. Cmdr. Lee Boone, chief of the compliance department, U.S. Coast Guard, Baltimore, said his service "lives homeland security every day," in intimate contact with DHS and many of its chief constituents: Transportation Security Administration (TSA), U.S. Customs and Border Protection, Immigration, FBI, first responders — essentially the same interlocking panoply of which Sheid spoke.

"We rely heavily on partnerships to carry out our mission since we're a small service," said Boone. He outlined vessel-boarding procedures, and the many complex data-sharing links that tie agencies together in multiple ways. Adding to the complexities, the 12-year Coast Guard officer stressed, the sea service's tasks must "balance security with [civil] liberties"— both at his Baltimore district and other busy American ports.

Much of Boone's work involves "increasing maritime awareness—awareness of assets, vulnerabilities, special hazards in port, locations of facilities and vessels."

These initiatives, he said, are all aimed at "intercepting threats well before they reach our shores."

Recent Coast Guard accomplishments, Boone said, include meeting the "red-letter day" of July 1, 2004, when the International Ship and Port Facility Security Code (ISPFS) went into force. Announced in 2002, the code required the United States and other participating countries to deploy inspectors to one another's ports, ensuring compliance with its security mandates.

On this end, every foreign ship making its first trip is boarded, and ships of nations that haven't signed on to ISPFS are tracked. The Coast Guard could deny entry to vessels from noncompliant countries, as well as intrusively inspect them at sea and take other measures, Boone explained. The ISPFS agreement falls under the United Nations International Maritime Organization.

The Container Security Imitative (CSI) is another program Boone cited as highly useful in helping the Coast Guard secure and speed maritime commerce. Although a product of the Bureau of Customs and Border Protection (CBP), the two agencies work closely on it. CSI includes 96-hour advanced notice of arrival for all 300-ton-and-greater incoming vessels from abroad. Each, Boone pointed out, must give ports-of-call, state flag, cargo manifests and lots of other data.

Undertaken in coordination with about two dozen nations to date, CSI, similar to ISPFS, involves "exchanges." U.S. officials are stationed abroad to work with foreign counterparts and vice versa. The aim is to secure the supply chain before cargoes are loaded.

CIS outlines punitive measures if goods turn out to be suspect. It also covers, to a degree, certification of security personnel. As with similar initiatives, CIS permits berthing denials, interceptions by Coast Guard cutters, and other actions. Such interlaced, proactive measures are vital, specialists said, because in many countries port security is slapdash.

The Coast Guard must help implement mandates under CIS, MTSA and ISPFS for vessel I.D. and port safety/security compliance. "You might be thinking this is a huge burden for the maritime industry — and you're right: $7 to 10 billion over the next 10 years," Boone said, adding that the private sector must contend with "huge amounts of policy and regulations" to pass multiple kinds of port security assessments — all of them a costly and time-consuming result of 9/11.

MTSA IMPLEMENTATION

Reserve Navy Lt. Cdr. Kevin Krick, senior adviser in maritime policy to the U.S. Maritime Administration (MARAD), helped draft the MTSA. His organization works most closely with the Coast Guard and is also active in the MTSA's vessel identification requirements.

MARAD also is instrumental in certification courses for various levels and kinds of maritime security personnel. Individual graduates coordinate with a ship's security officer, local law enforcement and military police, among others. Given the disparate organizations seeking guidance and certification, a large part of MARAD's mission was to "bring these people up to speed" with proper ship and maritime industry safeguard procedures, Krick said.

While highly professional in their own realms, they typically aren't steeped in requirements in "this specific maritime environment." Seeing this, and hearing industry and mariners' calls for standardization, "We created a MARAD/Coast Guard/MTSA109 Committee," said Krick.