

May 2006

**U.S. VIRTUAL SEA BORDER™ PROJECT PROPOSAL  
(Draft)**

**PURPOSE:** CREATE A U.S. VIRTUAL SEA BORDER™ (*"ANOTHER TOOL FOR THE U.S. PORT SECURITY THREAT ASSESSMENT TOOL BOX"*)

**GOAL:** LEVERAGE DEVELOPING SHIPBOARD INTERNET APPLICATIONS TO PERFORM REMOTE ALL-HAZARDS THREAT AUDITS OF ARRIVING FOREIGN SHIPS, INCLUDING SHIP MANAGEMENT, OWNERSHIP, AND THE ARRIVAL TERMINAL OPERATOR AND OWNER,

**OBJECTIVE:** PROVIDE LEGITIMATE OPERATORS WITH AN ECONOMIC INCENTIVE (MARITIME GREEN LANE ACCESS) TO BE OPERATIONALLY TRANSPARENT AND STRICTLY COMPLIANT.

Project Lead: TBD

Proposed Project Team: NI2 Center for Infrastructure Expertise (CIE)  
University Maine, Computer Systems  
U.S. Department of Homeland Security  
U.S. Coast Guard, Sector Northern New England  
U.S. Customs and Border Patrol, Portland, ME  
Ports of Portland / S. Portland, ME  
University of New Hampshire, Systems Engineering  
Teekay Shipping (Canada) Ltd.

Project Manager: Dale Ferriere, NI2-CIE Deputy Director

Budget: Proof of concept \$15,000 (NIST Grant)

**Vulnerability:** Because current U.S. port and cargo threat and risk assessment protocols do not address the entire marine industry enterprise (i.e., how U.S. marine terminals are owned, operated, managed, manned, maintained and how foreign-flagged commercial ships are owned, operated, managed, crewed, maintained, chartered) U.S. port security officials' capability to ensure comprehensive port and cargo security lacks effectiveness.

**Summary:** Although efforts to screen foreign-flagged ship arrivals into the U.S. and understanding of marine terminal operator and ownership relationships are improving, legitimate marine companies and their foreign ownership are consistently treated as potential terrorists and/or criminals, causing significant and unnecessary commercial delays, resulting in increased costs associated with the U.S. import of strategic cargoes.

**References:** The following references emphasize the need for improving information sharing and U.S. maritime domain awareness (MDA) with international entities:

## National Infrastructure Institute (NI2) Center for Infrastructure Expertise

- [GAO Report GAO-05-394](#) "Maritime Security: New Structures Have Improved Information Sharing, but Security Clearance Processing Requires Further Attention" Government Accountability Office; 04/15/2005 (Emphasized the need for information sharing amongst U.S. port security stakeholders);
- [Maritime Infrastructure Recovery Plan 2006](#) (International Outreach Strategy); and,
- [Homeland Security Presidential Directive 13: "National Strategy for Maritime Security"](#) (Improve MDA: Enhance international relationship and promote integration of U.S. allies and international and private sector partners into an improved global maritime security framework to advance common security interests in the Maritime Domain).

Since September 11, 2001, the Master of an arriving foreign-flagged ship is submitting a 96-hour pre-arrival notice, which includes information about the ship's administration (owner, operator, manager, flag state, classification society), cargo type, last port of call, next port of call, port state control boarding history, etc. From the time when the notice of arrival report is received by a centralized data base, Ship Arrival Notification System (SANS) and its e-component (e-NOAD: electronic notice of arrival / departure), information about the ship is distributed to the arrival port's U.S. Coast Guard Captain of the Port's office for assessment. Other agencies, such as U.S. Customs and Border Patrol, U.S. Immigration and Customs Enforcement, and the National Vessel Movement Center, are also separately (*working in stove pipes*) interpreting the ship's notice of arrival information.

This static threat assessment about the arriving foreign ship is completed by inputting arrival information data onto a spreadsheet, assigning numeric weights to each category, and determining whether or not to board the ship at sea for the purpose of performing a thorough and time-consuming law enforcement sweep (looking for weapons, contraband, and stowaways) before allowing it port entry. Never in this process, however, do the U.S. Port Officials (U.S. Coast Guard and/or U.S. Customs) gain dynamic access to critical information and key behind-the-scenes representatives about the entire marine industry enterprise (e.g., how the ship is owned, managed, crewed, maintained, regulatory compliance culture of the shipping company, screening process for newly hired seafarers, chartered and financed). Similarly, U.S. Port Officials do not always have the dynamic opportunity to interact with foreign owners of U.S.-based marine terminal operations.

**Proposed Solution:** The U.S. Port Officials' all-hazards threat assessment capability needs improvement in order to dynamically assess the overall risk (including terrorism) presented by foreign ships, their cargoes, their crews, their ship managers, their owners (financial backing for the ship), their commercial charter, and the associated marine terminal operator and owner. The successful port security interactive all-hazards threat assessment process would determine not only specific pre-arrival information about the ship, its cargo and its crew, but also audit the ship's management, financial management, and commercial charter as well. Additionally, the comprehensive port security all-hazards threat assessment process would include the owner of the marine terminal operation where that ship will moor and execute cargo operations.

## National Infrastructure Institute (NI2) Center for Infrastructure Expertise

Leveraging INTERNET, SATELLITE and BIOMETRIC technologies; creating an interactive all-hazards port security threat assessment process; developing a detailed list of audit questions from which key behind-the-scenes shipping and marine terminal representatives would be voluntarily asked to answer; and designing decision-support system software to analyze audit results is such a process. A U.S. virtual port security all-hazards threat assessment process could be created from which an arriving foreign-flagged ship, its management, cargo consignee or ship charter and marine terminal operator and owner are given the opportunity to voluntarily link with U.S. Port Officials via a world-wide-web application that includes adequate satellite bandwidth providing live video / audio in addition to text communications. With applicable stake-holders on-line, using prepared audit questions, a remote and acute all-hazards threat assessment by U.S. port officials is performed.

Suggested sample questions could:

- (a) Determine how seafarers and waterfront workers are screened and hired by the ship management and terminal management;
- (b) Whether or not the ship and/or marine terminal is, on behalf of their ownership groups, exclusively managed;
- (c) Whether or not seafarers hired to crew the ship are exclusive to that shipping company and/or waterfront workers hired to operate terminal equipment are exclusive to that marine terminal;
- (d) Whether or not the ship's ownership is a recognized, legitimate shipping company or has been subjected to several and spurious ownership schemes;
- (e) Whether or not the terminal's ownership is a recognized, legitimate terminal operator or has been subject to several and spurious ownership schemes; and,
- (f) Whether or not the commercial organization(s) chartering the ship to lift its cargo interests are similarly recognized as legitimate commercial ventures.

**Benefits:** If implemented, this all-hazards threat audit process makes the marine transport of goods more efficient and transparent. More effective than when an international airliner receives clearance to enter U.S. air space, the participating foreign-flagged ship, based on the U.S. Port Officials' assessment of the completed threat audit, would be given clearance to enter directly into a U.S. Port (via "Green Lane access"). Surveys strongly suggest that legitimate ship owners, cargo consignees or charters, and terminal operators and owners are willing to voluntarily participate and answer any and all U.S. Port Official questions, especially while the ship is at sea, rather than it being subjected to a pre-port entry law enforcement sweep and associated delay. In essence, the entire marine industry enterprise (ship, terminal, management, charter, operator and owner) could be more acutely screened by U.S. Port Officials, and a more comprehensive database about the marine industry enterprise created. Additionally, law enforcement assets are freed to address less-than-transparent marine operators.

This all-hazards threat audit process would permit ships and marine terminals from participating legitimate "white hat" shipping companies and marine terminal corporations to be identified and given access to a "maritime green lane", enabling them to optimize in-port time for cargo operations. This all-hazards threat audit process would also permit international owners of marine terminal operations and merchant ships to be part of the U.S. port security solution instead of being viewed with suspicion. More importantly, by implementing this process, it establishes a U.S. "virtual sea border,"

## National Infrastructure Institute (NI2) Center for Infrastructure Expertise

where the entire marine industry enterprise associated with that foreign-flag ship's arrival could be remotely audited. Lastly, shipping/chartering companies and marine terminal representatives would be dissuaded from submitting false or incomplete information because doing so subjects them to 18 USC Sec. 1001 criminal violations (falsifying information to U.S. federal officials) and potential civil liabilities in the event falsified information leads to loss of life or property damages stemming from a terrorist incident or marine casualty.

**Conclusion:** The U.S. Department of Homeland Security's (DHS) ongoing practice of using a static risk assessment process when determining whether or not to deploy a finite set of maritime law enforcement assets to perform at-sea law enforcement sweeps of ships managed and chartered by proven legitimate foreign-based shipping and chartering corporations creates unnecessary and time-consuming delays. Although this approach offers a deterrent, it does not effectively address the overall actual threat presented by an arriving foreign-flagged ship and the marine terminal where the ship moors. To improve U.S. Port Security Officials screening capabilities, regulators and port officials need to take a holistic approach about all threats from an arriving foreign-flagged merchant ship and the marine terminal operation by scrutinizing key behind-the-scenes parties intimately involved with the marine industry enterprise. By implementing a remote web-based all-hazards threat audit process of key behind-the-scenes parties, and creating an incentive for transparency by rewarding legitimate shipping and chartering companies and marine terminals with access to the "maritime green lane," the U.S. Virtual Sea Border process provides the United States with the opportunity to improve port security and simultaneously enhance maritime commerce.

---

This work was performed under the sponsorship of the U.S. Department of Commerce, National Institute of Standards and Technology. The intellectual property associated with this proposal is protected by U.S. law and therefore should be kept in strictest confidence between the sender and receiver of the document. By reading this document you hereby agree not to disclose its contents without approval from its author.