Challenges Measuring the Security and Resilience of the Marine Transportation System
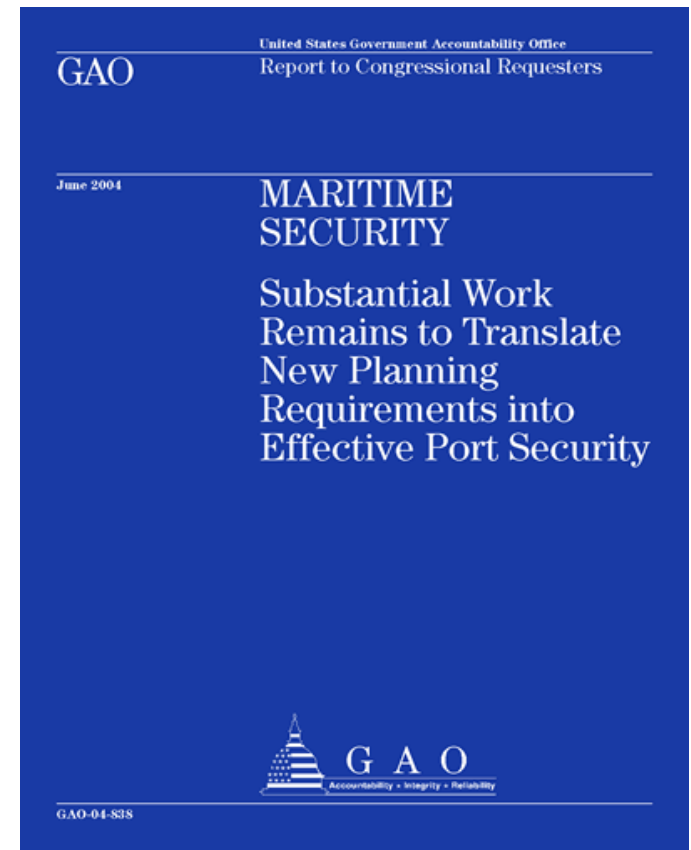
Stephen L. Caldwell
Director, Maritime Security Issues
U.S. Government Accountability Office

Diagnosing the Marine Transportation System
Transportation Research Board
National Academies of Science
Washington, DC, June 27, 2012

AGENDA

- Background
- Risk Management
- Port Security
- Container Security
- Port Resilience
- Conclusions
- Questions & GAO Contact

United States Government Accountability Office
GAO   Report to Congressional Requesters

June 2004

MARITIME SECURITY

Substantial Work Remains to Translate New Planning Requirements into Effective Port Security

GAO

GAO-04-838

BACKGROUND
Importance of U.S. Ports

- Ports contain many types/sectors of critical infrastructure.

- More than 95% of non-North American foreign trade arrives through U.S. ports.

- Ports are major centers for chemical and petroleum production activities.

- There are 17 strategic ports necessary for major military deployments.

- Many ports feature important national symbols (e.g., the Statue of Liberty).

- Recreation is a central feature of many ports.

BACKGROUND
Vulnerability of U.S. Ports

- Ports are extensive in size, and are accessible by water, land, and air.

- Many ports are intertwined with major urban areas.

- Ports process a large volume of cargo, passengers, and hazardous materials.

- Ports are a hub of activity for multiple transportation modes.

- Many vessels move through ports with relative anonymity.

- Cargoes move quickly due to just-in-time delivery systems.
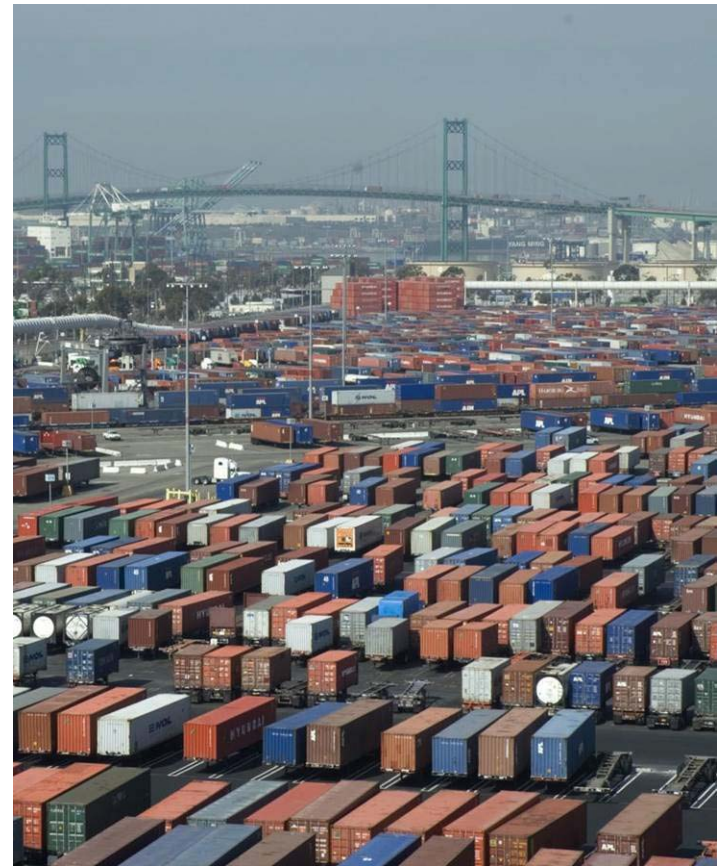
BACKGROUND
Importance of Containers

- Containers have revolutionized global trade, allowing fast and efficient transport of items around the world.

- Containers have created—and made us dependent upon—"just-in-time" supply chain logistics systems.

- Much foreign trade arrives in the 9-12 million containers that enter the United States every year.

- Terrorist incidents involving containers could close one or more ports, with serious repercussions for the military and economic activity in such ports and the nation as a whole.

BACKGROUND
Vulnerability of Containers

- Containers can be filled overseas at many different locations and are transported through complex logistics networks before reaching U.S. ports.

- Every time responsibility for cargo in containers changes hands along the supply chain there is the potential for a security breach.

- Criminal networks have exploited containers to smuggle people, drugs, weapons and other contraband.

- While CBP has maintained that the likelihood of smuggling WMD into the United States in cargo containers is relatively low, the consequence of such an action could be devastating.

BACKGROUND
Port Threats and Possible Scenarios

- Generally no known, credible threats in US, but overseas attacks have occurred:
  - USS Cole attack, Yemen,
  - Limberg Attack, Yemen,
  - Ferry Attack, Philippines,
  - Khawr Al Amaya Oil Terminal, Iraq.
- Possible U.S. Threats Include:
  - Entry point for terrorists or dangerous contraband (e.g., WMD),
  - Waterside facilities or port infrastructure could be attacked via small boat, or other means,
  - Possible targets include cruise ships, passenger ferries, military vessels and infrastructure.

BACKGROUND
## U.S. Government Accountability Office (GAO)

- GAO is an independent, nonpartisan agency that works for the U.S. Congress.

- The GAO mission is to support the Congress in meeting its oversight responsibilities and to help improve the performance and ensure the accountability of the federal government.

- GAO evaluates how the federal government manages programs and spends funds.

- Regarding maritime issues, since 9/11, GAO has issued over 75 reports on maritime and supply chain security.

RISK MANAGEMENT
Risk Management Defined

- Risk Management is the continuous process of assessing risks, reducing the potential that an adverse event will occur, and putting steps in place to deal with any event that does occur.

- It has five major phases:
  - Setting strategic goals and objectives, and determining constraints.
  - Assessing risks.
  - Evaluating alternatives for addressing risks.
  - Selecting appropriate alternatives.
  - Implementing alternatives and monitoring progress and results.

Source: GAO.

9
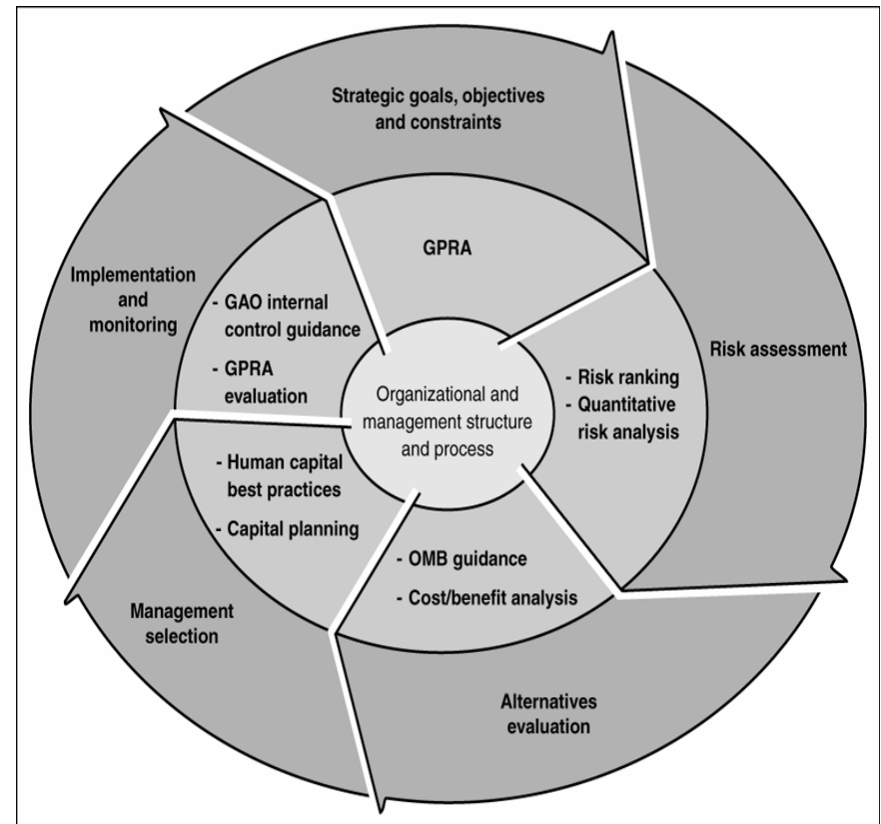
RISK MANAGEMENT
Inherent Challenges Measuring Security Risk

- GAO reviewed early DHS risk management efforts (GAO-06-91).

- Compared to other risks, there are inherent challenges in measuring deterrence & intentions of an adaptive terrorist threat.

- Some related limitations are:
    - Threat-related data
    - Vulnerability-related data
    - Consequences-related data

- Difficulty comparing and prioritizing risk across different assets in a port, across ports, across other transportation sector assets, and across other sectors nationwide.

RISK MANAGEMENT
USCG MSRAM Tool Limitations Measuring Risk

GAO reviewed USCG Maritime Security Risk Analysis Model, or MSRAM (GAO-12-14).

- MSRAM is one of better tools we have evaluated, but…

- Focuses only on security (vs. USCG non-security missions).

- Cannot model the adaptive - intelligent adversary, or network - system effects.

- Overall complexity of tool to properly train staff, get good data, and do the analysis.

- Subjectivity of data (for threat, vulnerability, and consequences).

RISK MANAGEMENT
USCG MSRAM Tool Limitations in Energy Sector

GAO reviewed risks to maritime energy supply chain security (GAO-11-883T).

Data challenges negatively impact DHS

- Lack of explicit performance measures for emergency response capability in event of an attack.

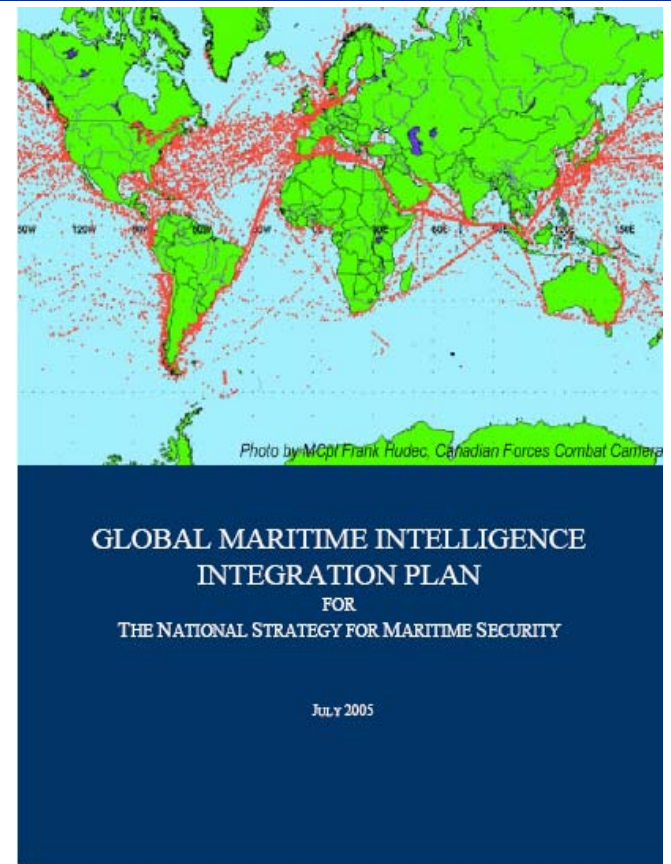Additional USCG challenges with MSRAM where there is lack of…

- Vulnerability-related data regarding hardness of potential targets.
- Consequences-related data regarding secondary economic impacts.

PORT SECURITY
Examples of Port Security Programs

- USCG (and other agencies) developed national-level strategies and subordinate plans (see slide right), as well as port-specific security committees and plans.

- USCG approval of vessel/facility security plans, and inspections to ensure these plans are being implemented by vessels/facilities.

- USCG port state control inspections of incoming foreign and "high interest vessels" and (with CBP) checks foreign seafarers.

- USCG maritime security response operations (e.g., to patrol infrastructure and escort higher risk target vessels).

- FEMA administers Port Security Grant Program to fund state/local/private projects that improve maritime security.

Photo by MCpl Frank Hudec, Canadian Forces Combat Camera

GLOBAL MARITIME INTELLIGENCE
INTEGRATION PLAN
FOR
THE NATIONAL STRATEGY FOR MARITIME SECURITY

JULY 2005

PORT SECURITY
USCG Inspections of Shore and Offshore Facilities

- GAO reviewed USCG inspections of both shore & offshore facilities (GAO-08-12, GAO-12-37).

- Onshore 3,200+ terminals, chemical plans, factories, and power plants; and offshore 50+ drilling rigs & other infrastructure.

  - GAO unable to determine the extent to which Coast Guard had met shore inspection requirements.

  - There was incomplete / duplicate data in compliance database and lack of documentation for annual exams and spot checks.

PORT SECURITY
## USCG and CBP Security Controls for Foreign Seafarers

- GAO reviewed USCG/CBP vetting of foreign seafarers (GAO-11-195).

- Millions of foreign seafarers that arrive on cruise ships and cargo ships and pose potential threats as terrorists, absconders and deserters.

- USCG and CBP are responsible for preventing illegal immigration and identifying individuals who are potential security risks.

- GAO found data reliability concerns in information DHS uses to inform strategic and tactical plans.

- GAO found discrepancies within and between USCG/CBP on absconders and deserters (see next slide).

PORT SECURITY
USCG and CBP Weak Data on Foreign Seafarers
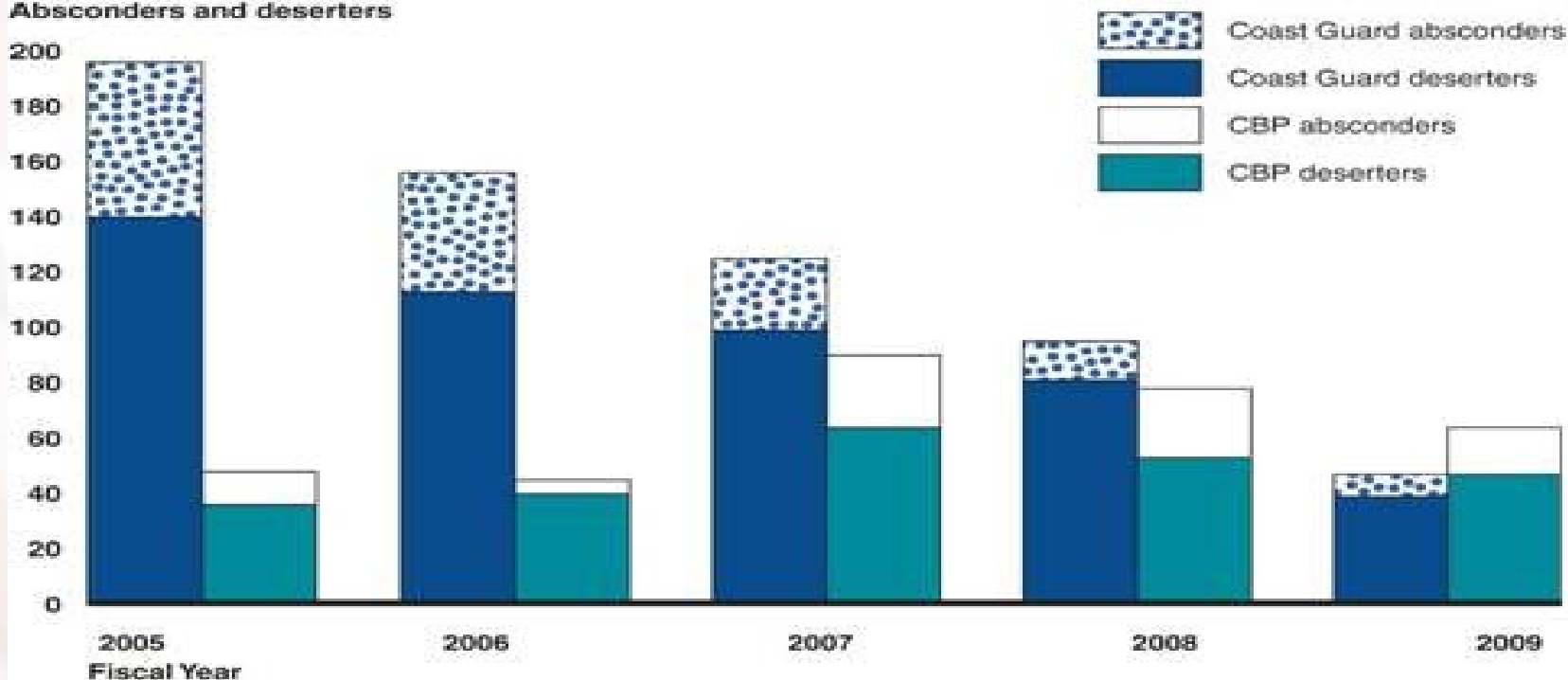
Source: GAO analysis of Coast Guard ICC and CBP data.

PORT SECURITY
USCG Metric on Percent of Risk Reduction

- GAO reviewed USCG metric for reducing maritime security risk (GAO-12-14).

- USCG has proxy "outcome" measure of the percent reduction in risk due to, among other things, its Maritime Security Response Operations (e.g., vessel escorts, shore side patrols).

- Starts with "raw" risk, then SMEs estimate probability that USCG security regimes will prevent successful attacks (16 scenarios).

- USCG reports the result, but generally does not use it for decision making on resources or operations.

PORT SECURITY
FEMA Port Security Grant Program (PSGP)

Funds Drawn Down	Available Funds	Unavailable Funds
$394.8 million (23.6%)	$873.4 million (52.1%)	$407.8 million (24.3%)

Source: GAO analysis of FEMA data as of September 2011.

PORT SECURITY
FEMA Port Security Grant Program (continued)

- GAO twice reviewed management of PSGP (GAO-06-91 & GAO-12-47).

- FY2006-2010, DHS awarded $1.7 billion in PSGP funds to ports. Many funds remain unspent (see previous slide).

- Multi-step process but, in general, PSGP grant award based on port risk determined by MSRAM / other factors.

- Vulnerability part of formula is not responsive to PSGP funded improvements in port security.

- In both 2006 and 2012 reports, GAO found PSGP has no performance measures in place, and recommended that such measures be developed.

CONTAINER SECURITY
Examples of Container Security Programs

- DHS issued a national strategy for global supply chain security.

- CBP uses Automated Targeting System (ATS) to identify potentially high-risk containers for further scrutiny.

- CBP places officers overseas to work with host customs to identify and scan high risk containers before loading.

- CBP developed Secure Freight Initiative to pilot scanning 100% of inbound container before loading.

- CBP partnered with private sector in Customs Trade Partnership Against Terrorism to improve security.

- CBP partnered with World Customs Organization to develop international standards for supply chain security.

STRATEGY TO ENHANCE
INTERNATIONAL SUPPLY CHAIN SECURITY

JULY 2007

CONTAINER SECURITY
Automated Targeting System (ATS)

- GAO twice reviewed ATS, which is used to identify high-risk containers (GAO-06-591T & GAO-10-841).

- Data quality is critical, and CBP implementation of the "10+2 rule" provided more accurate and complete cargo data for ATS to analyze.

- CBP has also used vessel stow plans (new from the10+2 rule) to identify incorrectly manifested containers, which are inherently high-risk because of omissions in their origin or contents.

- However, our earlier review found that CBP could not measure the effectiveness of ATS in targeting the highest risk containers. GAO has ongoing review to evaluate CBP's progress in this area.
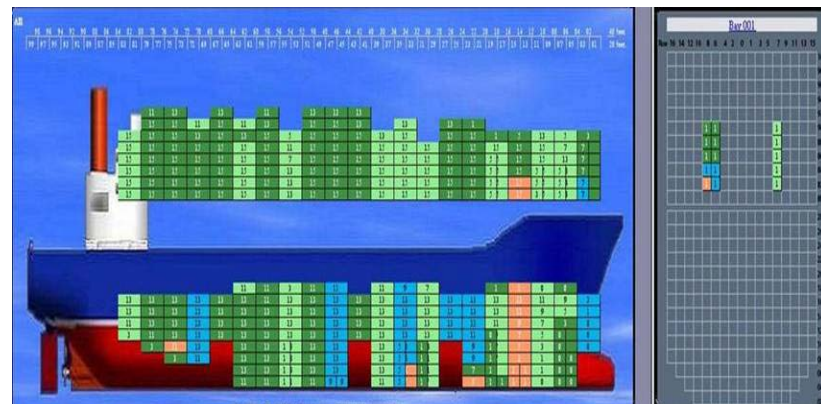
CONTAINER SECURITY
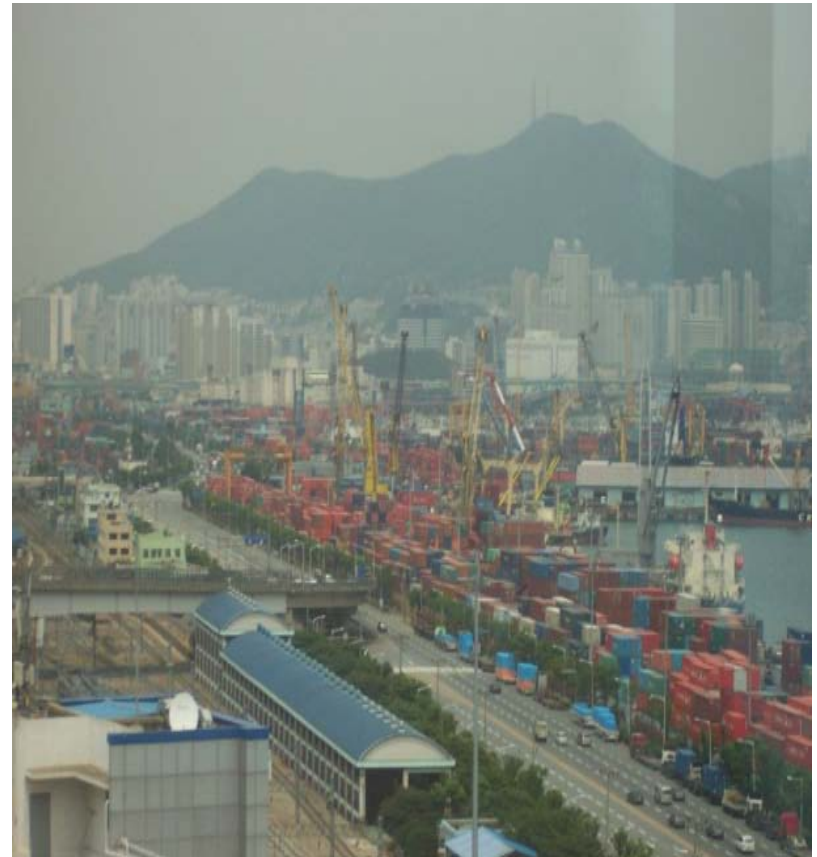
Container Security Initiative (CSI)

- GAO twice reviewed CSI program (GAO-05-557 & GAO-08-187).

- The CSI places CBP officers in 58 foreign ports to work with host nations to identify and scan high risk US-bound containers.

- Examination of high-risk cargo has increased, but challenges remain including

  - CBP lacks technical data and process evaluations to ensure the fidelity of host government inspections.

- CBP faces challenges developing outcome-oriented performance measures on the results of CSI at the port or program level.

CONTAINER SECURITY
## Secure Freight Initiative (SFI)

- GAO twice reviewed 100% scanning and SFI issues (GAO-08-533T and GAO-10-12).

- CBP developed Secure Freight Initiative (SFI) due to statutory mandate to scan 100% of US-bound containers with two types of scanners (NII and RPM).

- Multiple challenges encountered, including congestion -- difficult to measure intermodal congestion in affected ports (see slide on right).

- CBP was able to measure progress toward meeting 100% goal in five pilot ports (see next slide).

Container Security
Secure Freight Initiative (continued)

Average percentage of U.S.-bound containers scanned during SFI program

- ☐ **Non-Intrusive Imaging (NII)**
- ■ **Radiation Portal Monitors (RPM)**
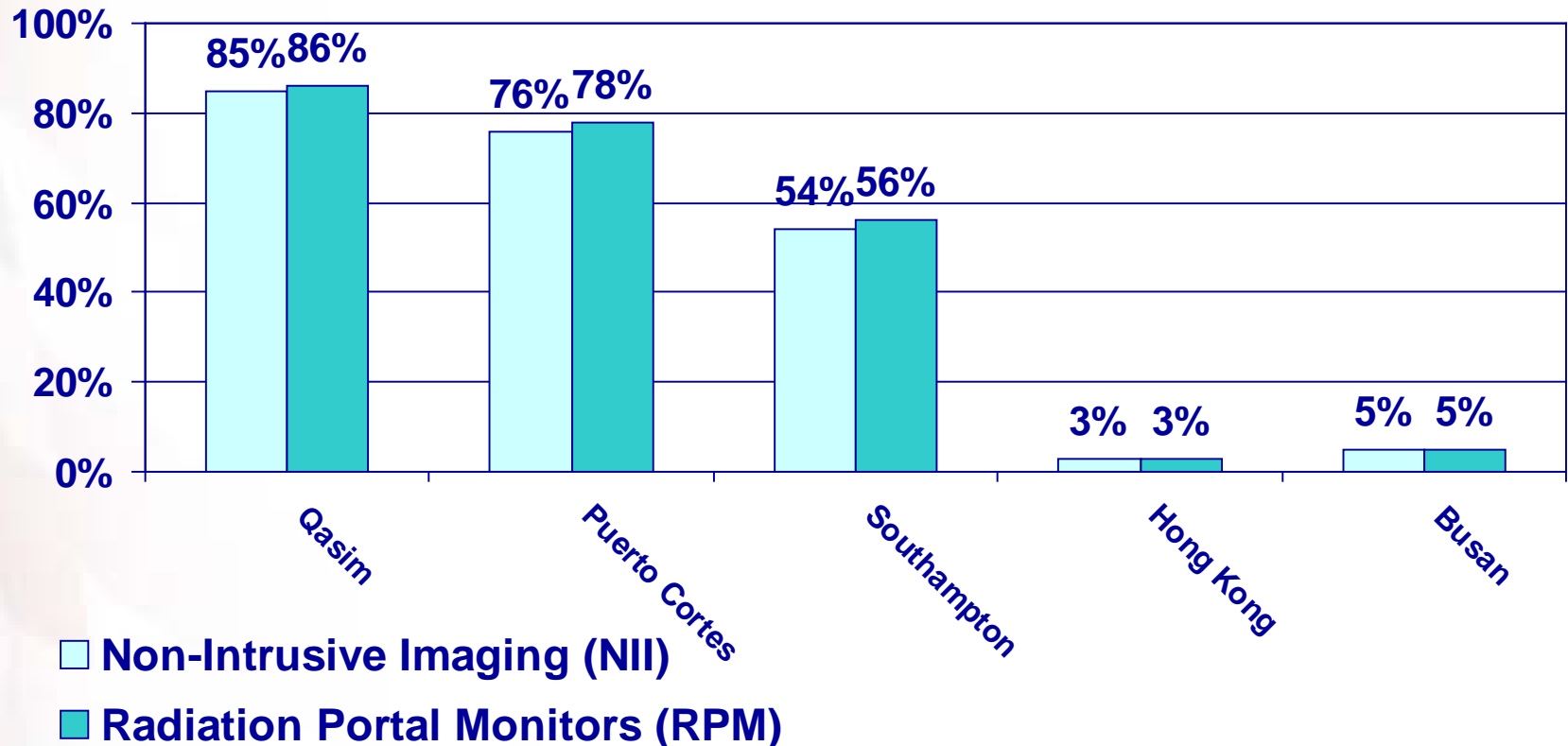
CONTAINER SECURITY
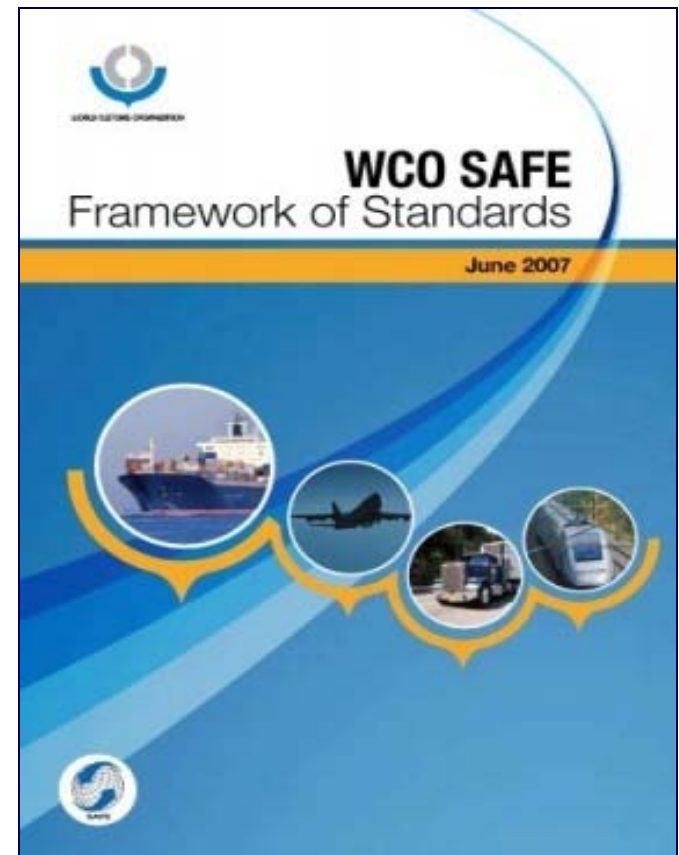## Customs Trade Partnership Against Terrorism (CTPAT)

- GAO twice reviewed CTPAT program (GAO-05-404 & GAO-08-240).
- Program is a CBP voluntary partnership with companies involved in oceangoing shipping to USA. Members companies provide CBP with security information and, in return, their cargo containers receives less scrutiny.
- Challenges:
  - It is difficult for CBP to measure the extent that member company security practices meet the minimum criteria.
  - Determining the extent to rely upon reviews by companies themselves or by third parties (e.g., ISO 28000 reviews).
  - Also, CBP has no performance measure to gauge company or broader improvements to security.

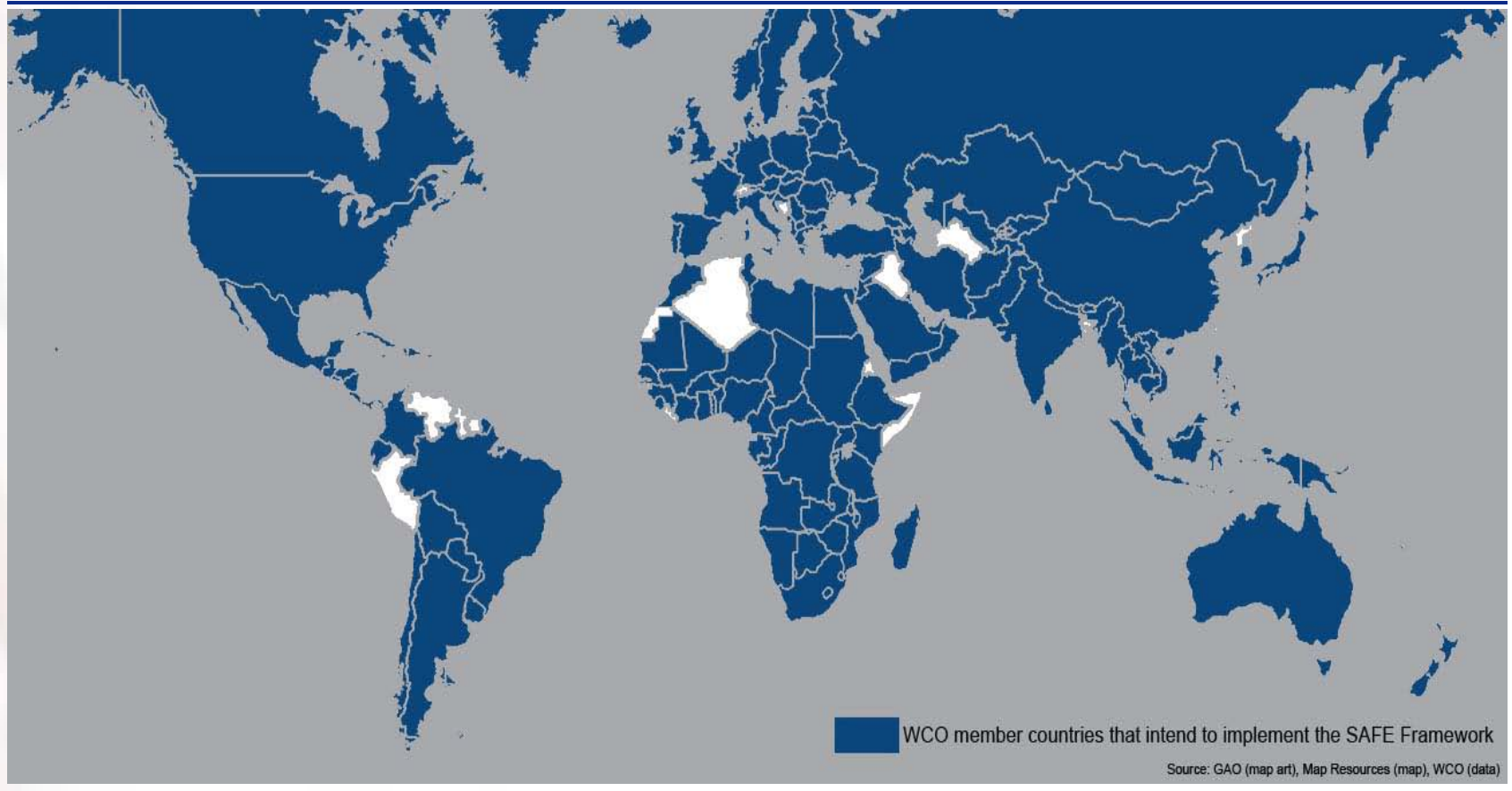**DP WORLD**

CONTAINER SECURITY
International Supply Chain Security Standards

- GAO reviewed CBP international cooperation efforts (GAO-08-538).

- CBP and World Customs Organization (WCO) developed SAFE Framework of international container security standards.

- SAFE has two pillars with from 6 to 11 standards each, and four core principles.

- Measuring effectiveness is a challenge with international standards because countries police themselves and self-report their results (see next slide).

- Same measurement challenge exists with International Maritime Organization (IMO) and its ISPS code for maritime security.

WCO SAFE
Framework of Standards
June 2007

CONTAINER SECURITY
Countries Intending to Adopt SAFE Framework (2008)

WCO member countries that intend to implement the SAFE Framework

Source: GAO (map art), Map Resources (map), WCO (data)

PORT RESILIENCE
Definition of Resilience

- GAO reviewed efforts to define and promote resilience of critical infrastructure (GAO-10-296).

- The concepts associated with resilience (including recovery, reconstitution, and continuity of operations) have evolved over the years.

- The National Infrastructure Protection Plan defined resilience as the ability to resist, absorb, recover from, or successfully adapt to adversity or a change in conditions.

- GAO found that both the national plan and some sector-specific plans had been revised to incorporate resilience.

National Infrastructure Protection Plan

Partnering to enhance protection and resiliency

2009

PORT RESILIENCE
Examples of Resilience Related Programs

- USCG (and others) developed National Maritime Infrastructure Recovery Plan. New National Strategy for Global Supply Chain Security emphasizes resilience as one of two main goals.

- USCG requires Area Maritime Security Plans to include a recovery and salvage component, and FEMA PSGP program requires key ports to have Port-wide Risk Mitigation Plans.

- NPPD and its Protective Security Advisors provide resiliency advice to owners and operators of individual assets to improve their resiliency.

- NPPD and its Regional Resiliency Assessment Program examines regions and clusters of assets.

THE MARITIME INFRASTRUCTURE RECOVERY PLAN

FOR

THE NATIONAL STRATEGY FOR MARITIME SECURITY

APRIL 2006

PORT RESILIENCE
Port Recovery and Resilience

- GAO reviewed USCG port recovery planning (GAO-12-494R).

- Port level recovery planning was meeting key elements required by SAFE Port Act and USCG guidance, including maritime transportation recovery units, essential elements of Information, priority setting, and salvage response plans.

- But recovery is just one aspect of resiliency, and USCG authority with MTSA is limited to shore side facilities and infrastructure.

- GAO is conducting follow-on review on the broader issue of port resiliency (ongoing study 441074).

PORT RESILIENCE
Infrastructure Asset Resilience

- GAO reviewed NPPD program to promote resiliency of individual infrastructure assets (GAO-10-772).

- DHS has begun to increase its emphasis on resiliency in vulnerability and risk assessments.

- But DHS has not developed performance measures to ensure the effectiveness of owner and operator actions to address resiliency gaps.

- GAO is conducting follow-on review on NPPD's broader Regional Resiliency Assessment Program or RRAP (ongoing study 441074).

CONCLUSIONS

- There are inherent difficulties because terrorist attacks are relatively infrequent and defy statistical analysis common to other applications of risk management.

- Difficult to model some aspects (e.g., measuring deterrence and accounting for the intelligent/adaptive adversary and system/network effects).

- The quality of data on security programs can vary, hindering good measurement.

- There are certainly measures of security activities / outputs, but…

- There are few (if any) good measures of security results / outcomes.

QUESTIONS AND GAO CONTACT

Questions?

Stephen L. Caldwell, (202) 512-9610, email: caldwells@gao.gov

GAO website: www.gao.gov

BACK-UP SLIDE
International Framework for Container Security

- The World Customs Organization (WCO) and its SAFE Framework of Standards provides an international framework for container security.

- The SAFE Framework has two pillars and four core principles.

- Reference: GAO-08-538 for larger graphic and more details.

WCO SAFE Framework of Standards

Customs-to-Customs Standards
1. Integrated supply chain management
2. Cargo inspection authority
3. Modern technology inspection equipment
4. Risk-management systems
5. High-risk cargo or container
6. Advance electronic information
7. Targeting and communication
8. Performance measures
9. Security assesssments
10. Employee integrity
11. Outbound security inspections

Customs-to-Business Standards
1. Partnership
2. Security
3. Authorization
4. Technology
5. Communication
6. Facilitation

First core principle: Standardization of advance electronic cargo information requirements for inbound, outbound, and transit shipments.

Second core principle: Commitment to the use of a consistent risk management approach to address security threats.

Third core principle: Performance of outbound inspection of high-risk containers and cargo by nation from which the cargo is shipped at reasonable request of receiving nation, preferably using nonintrusive inspection equipment.

Fourth core principle: Adoption of customs-to-business partnership program (such as the C-TPAT program).

BACK-UP SLIDES
International Maritime Organization and ISPS Code

International Maritime Organization
- Overall mission to improve and assure safety, environmental stewardship and security at sea.
- About 98 percent of world's shipping fleet operates under its various agreements.
- Worked with member states to amend SOLAS and issue International Ship and Port Facility Security (ISPS) code.
- ISPS code is performance-based, not standard-based.
- ISPS code compliance based on country self-certification – IMO itself has no enforcement mechanism.

ISPS CODE
2003 Edition

International Ship & Port Facility Security Code
and SOLAS Amendments 2002

IMO
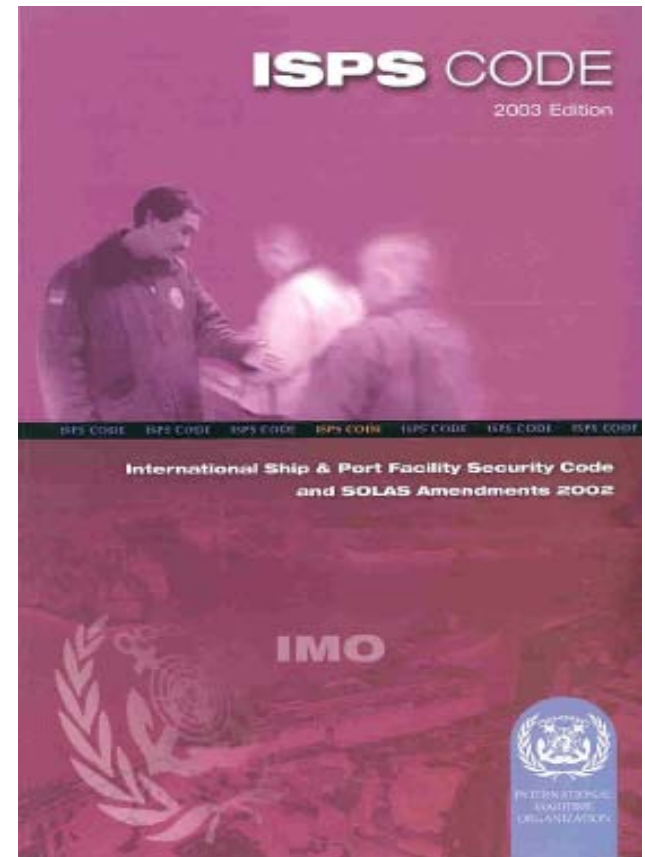
COPYRIGHT

Copyright
This is a work of the U.S. government and is not subject to copyright protection in the United States. The published product may be reproduced and distributed in its entirety without further permission from GAO. However, because this work may contain copyrighted images or other material, permission from the copyright holder may be necessary if you wish to reproduce this material separately.