

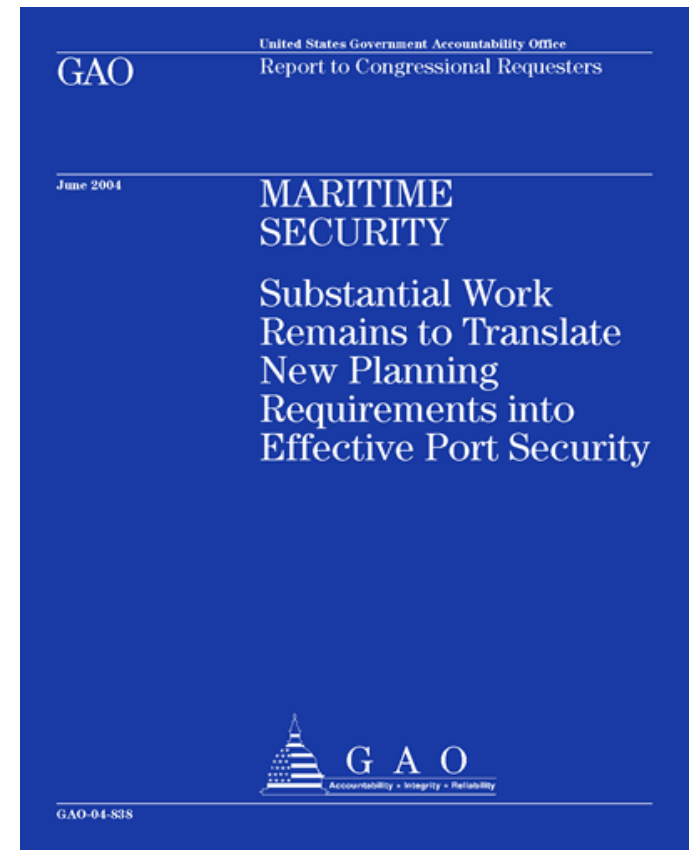
The Tenth Anniversary of MTSA: Progress and Enduring Challenges

Stephen L. Caldwell
Director, Maritime Security Issues
U.S. Government Accountability Office

Port Security Seminar
American Association of Port Authorities
Baltimore, MD, July 17, 2013

AGENDA

- Background
- Plans & Exercises
- Facilities, Vessels, People
- Cargo: Supply Chain Security
- Maritime Domain Awareness
- Enduring Challenges
- Conclusions on MTSA
- Ongoing Engagements
- Questions & GAO Contact



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 programs and spending
- Regarding maritime issues, since 9/11, GAO has issued over 75 reports on maritime and supply chain security
- NOTE: This briefing is a summary of GAO-12-1009T (which also has detailed appendices that reference other GAO reports)



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
- Recreation is a central feature of many ports
- Many ports feature important national symbols (e.g., the Statue of Liberty)



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 are a hub of activity for multiple transportation modes
- Many vessels move through ports with relative anonymity
- Ports process a large volume of cargo, passengers, and hazardous materials
 - Cargoes move quickly due to just-in-time delivery systems
 - About 9-12 million containers enter the United States every year



BACKGROUND

Key Maritime Transportation Security Statutes

Maritime Transportation Security Act (MTSA), 2002

- Enacted in response to 9/11 to address concerns over the security of U.S. ports and waterways
- Required a wide range of security improvements designed to help protect the nations ports, waterways, and coastal areas from terrorist attacks including planning, personnel security, and monitoring vessels and cargo
- Prior to 9/11, federal attention on ports focused on navigation and safety issues, such as dredging channels and environmental protection

Security and Accountability for Every (SAFE) Port Act of 2006

- Amended MTSA and codified many of the security improvement programs implemented in response to MTSA requirements
- Established interagency operational centers for port security, improved cargo screening standards, and provided incentives to importers to enhance security measures

BACKGROUND

Federal Roles and Responsibilities

DHS and its components have lead federal agency responsibilities for MTSA:

- **U.S. Coast Guard** – responsible for ensuring the safety and security of U.S maritime interests and leading homeland security efforts in the maritime domain
- **U.S. Customs and Border Patrol (CBP)** – responsible for screening incoming vessels' crew, passengers and cargo, while facilitating legitimate commerce
- **Transportation Security Administration (TSA)** – responsible for managing the Transportation Worker Identification Credential (TWIC) program, developed to limit access to regulated maritime facilities
- **Domestic Nuclear Detection Office (DNDO)** – responsible for acquiring and deploying radiation detection equipment at domestic ports to scan containers before they enter U.S. commerce
- **Federal Emergency Management Agency (FEMA)** – responsible for administering grants to improve security at highest-risk U.S. ports

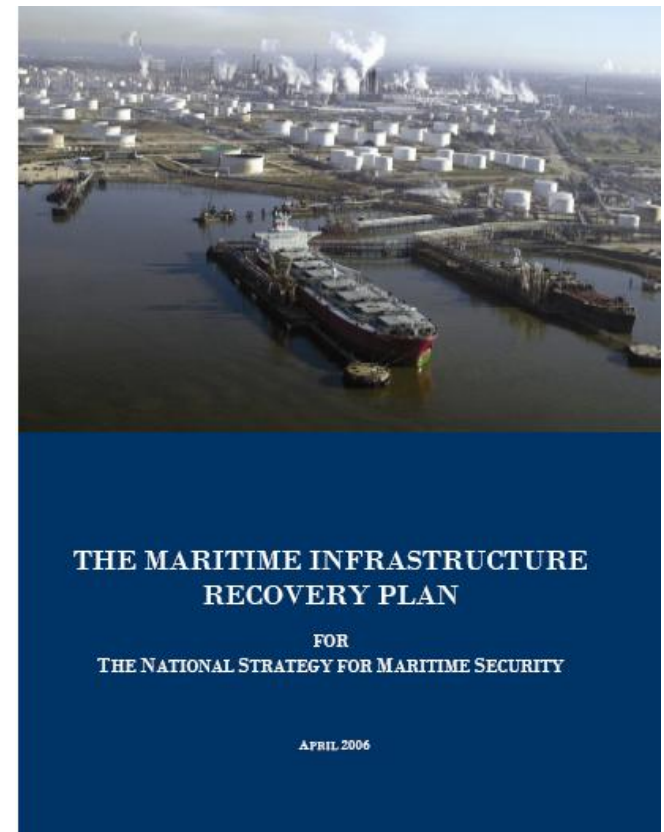
PLANS & EXERCISES

National-Level Security Planning

National Strategy for Maritime Security, 2005

- Developed jointly by the Secretaries of Defense and Homeland Security to establish a comprehensive strategy to enhance maritime security and defense
- Eight supporting plans intended to address the specific threats and challenges of the maritime environment (e.g., the Maritime Infrastructure Recovery Plan)
- GAO reported that these plans were generally well developed and, collectively, included
 - purpose, scope, and methodology
 - problem definition and risk assessment
 - organizational roles, responsibilities, and coordination
 - integration and implementation

Reference: GAO-08-672



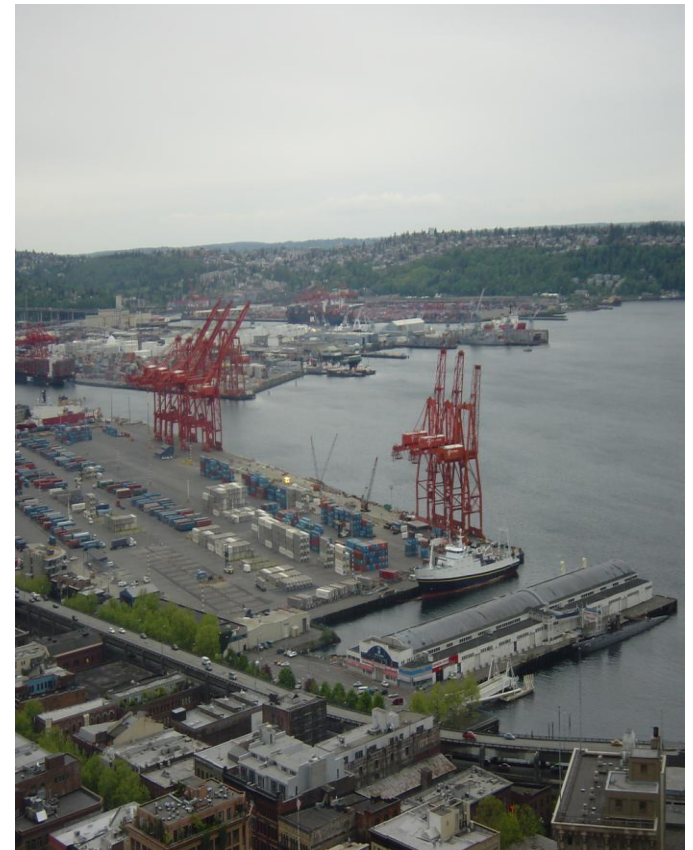
PLANS & EXERCISES

Port-Level Security Planning

Area Maritime Security Plans (AMSP)

- Developed by the Coast Guard for all 43 port areas with input from government and private entities to enhance the security of domestic ports
- Serve as the primary means to identify and coordinate Coast Guard procedures related to prevention, protection, and security response
- GAO work on AMSPs showed plans that
 - Focused on preventing terrorism
 - Included discussion on natural disasters with detailed information on plans for recovery
 - Incorporated key recovery and salvage response planning elements

Reference: GAO-07-412, GAO-08-126T, GAO-12-494R



PLANS & EXERCISES

Exercising Port-Level Security Plans

Exercising security plans

- Coast Guard and the Area Maritime Security Committee are required to conduct or participate in exercises to test AMSPs annually
- Several programs initiated to test security plans
 - Port Security Training Exercise Program
 - Area Maritime Security Training and Exercise Program
- GAO work showed that the Coast Guard has exercised the AMSPs, identified areas for improvement, and improved the timeliness and quality of after-action reports that include lessons learned

Reference: GAO-05-170, GAO-08-126T, GAO-12-37



FACILITIES, VESSELS, PEOPLE

Facility Security Plans and Inspections

- MTSA requires certain maritime facilities to develop security plans to mitigate facility security vulnerabilities
- Consistent with the SAFE Port Act, the Coast Guard conducts one announced and one unannounced inspection of these facilities each year (with some exceptions, all inspections on offshore energy facilities are announced in advance)
- GAO work showed that the Coast Guard
 - Identified and corrected port deficiencies in about one-third of the port facilities inspected
 - Took actions to help ensure the security of off-shore energy facilities (though not all required inspections were done)

Reference: GAO-08-12, GAO-12-37



FACILITIES, VESSELS, PEOPLE

Facilities and Port Security Grant Program

Port Security Grant Program (PSGP)

- Provides funding to state, localities, and private operators to strengthen port facilities against risks associated with terrorist attacks
- Administered by FEMA, but Coast Guard provides subject matter expertise to inform grant award decisions
- Total of \$2.4 billion funded, fiscal years 2003-2012
- In November 2011, GAO reported that
 - Funds allocated for fiscal years 2010 and 2011 were made largely based on risk
 - However, numerous challenges in getting funds out and evaluating improvements

Reference: GAO-06-91, GAO-12-47



FACILITIES, VESSELS, PEOPLE

Vessel Security Plans

Vessel plans and inspections

- MTSA requires certain vessel owners and operators to develop security plans to mitigate vessel security vulnerabilities
- The Coast Guard approves the vessel security plans and has taken steps to help vessel owner and operators comply with requirements:
 - Issuing guidance and establishing a “help desk”
 - Hiring contractors to provide expertise in reviewing initial vessel security plans
 - Conducting regular boardings and inspections of vessels to ensure compliance
- GAO work showed that the Coast Guard had
 - Identified and corrected deficiencies in vessel security plans
 - More recently, ensured plans included piracy annexes for vessels transiting high-risk areas

Reference: GAO-04-838, GAO-10-856



FACILITIES, VESSELS, PEOPLE

Boarding and Escorting Vessels

- The Coast Guard boards and escorts a certain percentage of high capacity passenger vessels to help ensure their security, such as:
 - Boarding foreign vessels as part of the Port State Control program, which is tied into Coast Guard's International Port Security Program (discussed later in the slides)
 - Escorting cruise ships, energy tankers, and ferries to show presence, provide deterrence, and help prevent attacks
 - Providing a security presence on passenger ferries
- Reference: GAO-08-141, GAO-10-400, GAO-11-207



FACILITIES, VESSELS, PEOPLE

Transportation Worker Identification Credential (TWIC)

- MTSA required DHS to issue biometric TWIC cards to control access to secure port areas
- TSA responsible for initial development and USCG later involved in testing and enforcing
- GAO reported that TSA and the Coast Guard
 - Enrolled over 93 percent of the estimated 1.2 million potential users by April 2009 deadline
 - But agencies face several challenges in fully implementing the TWIC program
 - Recent pilot tests could not determine if problems found were due to cards, readers, or the users
 - The program is still not the biometric-based program intended by Congress and originally designed by TSA

Reference: GAO-10-43, GAO-11-657, GAO-13-198



FACILITIES, VESSELS, PEOPLE

Screening Crews and ILO-185

- CBP and the Coast Guard screen information on vessel crews to assess risks:
 - Vast majority of crew screenings involve cruise ships because of their large crews (up to 3,000) and how they regularly swap crew members on and off
 - Extra scrutiny for vessels with a history of having invalid or incorrect crew manifest lists, or landing unlawful seafarers (absconders, stowaways)
 - Coast Guard may also conduct armed security boardings in cases where vessel or crew may present high risks
- International Labor Organization & ILO-185
 - ILO is specialized agency of the UN re: labor
 - ILO-185 on seafarers was adopted 2003, but is not widely ratified or implemented
 - US opposition to ILO-185 is largely based on allowance for seafarers to disembark without any visa required
- Reference: GAO-11-195

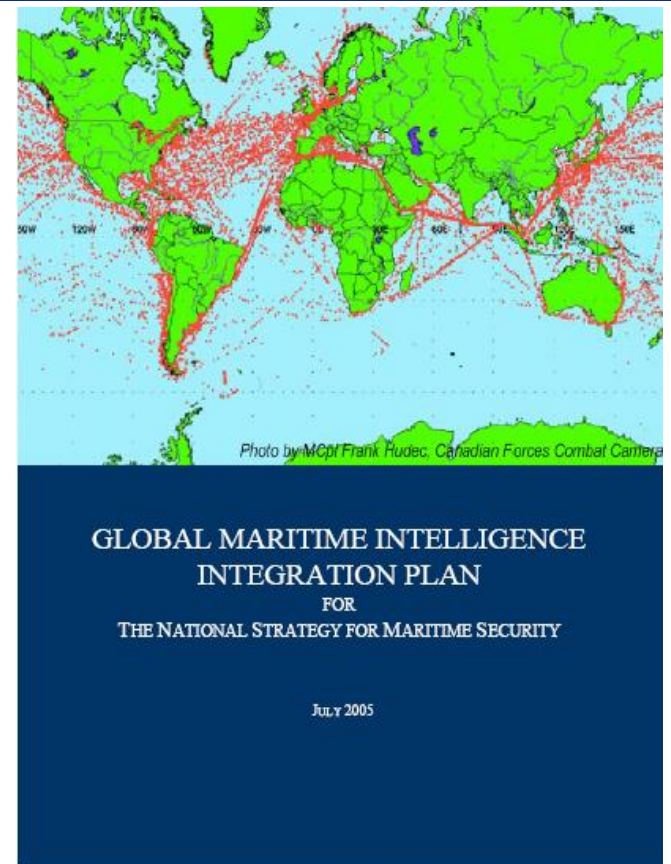


MARITIME DOMAIN AWARENESS

MDA & Risk Assessments

- MDA defined as the effective understanding of anything in the maritime environment that could impact the security, safety, economy or environment of the U.S. A key part of MDA is understanding risks
- Maritime Security Risk Analysis Model (MSRAM)
 - Coast Guard's primary tool for assessing and managing risks to assets in the maritime domain
 - Standardized way for assessing risk to infrastructure
 - Calculates risk based on scenarios in terms of threat, vulnerabilities, and consequences to maritime targets
- GAO reported that MSRAM aligns with DHS risk assessment criteria and that the Coast Guard
 - Made progress in assessing maritime security risk
 - Established a foundation for risk management ahead of other DHS components
 - Addressed limitations of its previous risk model

Reference: GAO-06-91, GAO-10-940T, GAO-12-14



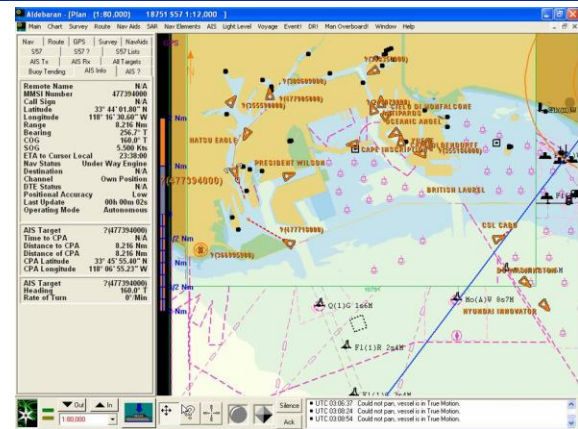
MARITIME DOMAIN AWARENESS

Vessel Tracking Systems

Vessel tracking systems

- MTSA and the Coast Guard and Maritime Transportation Act of 2004 require vessel tracking
- Coast Guard relies on several systems to track and assess the risk of vessels
 - Long-range identification and tracking systems for vessels at sea
 - Land-based automatic identification system for vessels in U.S. coast areas, inland waterways, and ports
- GAO has reported that the Coast Guard has
 - Developed vessel tracking systems that provide key information to identify and mitigate high-risk vessels
 - Taken actions to partner with local port entities to reduce costs and analyzed the performance of tracking systems to reduce duplication
 - But vessel tracking systems are generally not effective in tracking potentially threatening small vessels

Reference: GAO-02-477, GAO-04-868, GAO-09-337



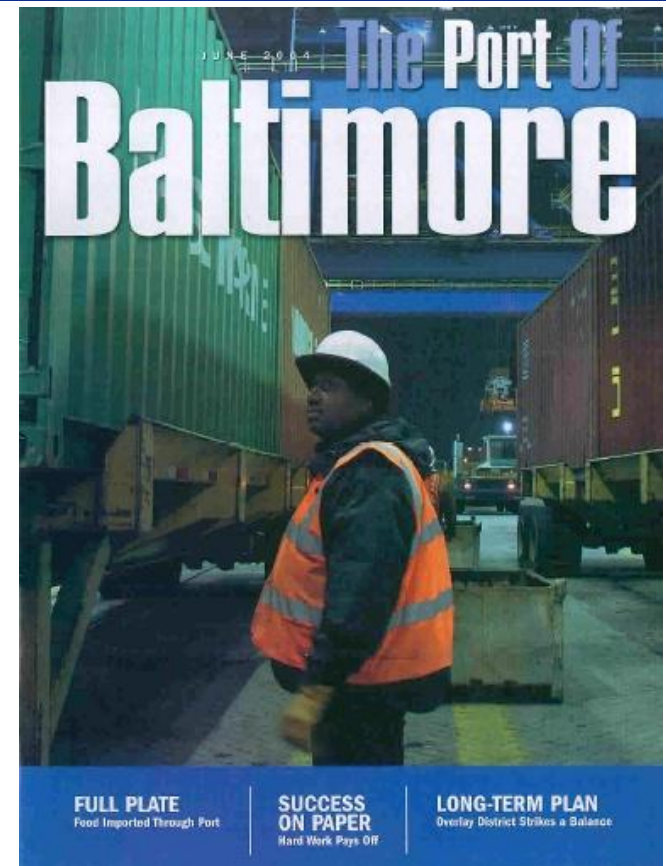
MARITIME DOMAIN AWARENESS

Info Sharing and Port-Level Committees

Area Maritime Security Committees (AMSCs)

- Required by Coast Guard regulations implementing MTSA
- AMSCs consist of members at all levels of government, the private sector, and other key port stakeholders who
 - May be affected by security policies
 - Share information and develop port security plans
- AMSCs help identify critical infrastructure and risks to the port, develop mitigation strategies for these risks, and communicate security information to port stakeholders
- GAO work showed that AMSCs
 - Improved information sharing among port stakeholders
 - Improved the timeliness, completeness, and usefulness of port security information

Reference: GAO-05-394, GAO-06-933T



MARITIME DOMAIN AWARENESS

Info Sharing and Interagency Operations Centers

Interagency Operations Centers (IOCs)

- Required by the SAFE Port Act and the Coast Guard Authorization Act of 2010
- Physical or virtual centers of collaboration to improve maritime domain awareness and operational coordination among port partners
- GAO work on IOCs showed
 - Early prototypes between DHS, DOD, and DOJ improved information sharing
 - Physical IOCs can provide continuous information about maritime activities and directly involve participating agencies in operational decisions
 - But Coast Guard has only made limited progress in expanding IOCs using a “virtual model” and other stakeholders have generally not participated in the related “watchkeeper” program
 - DHS only recently began to support IOC program

Reference: GAO-05-394, GAO-08-126T, GAO-12-202



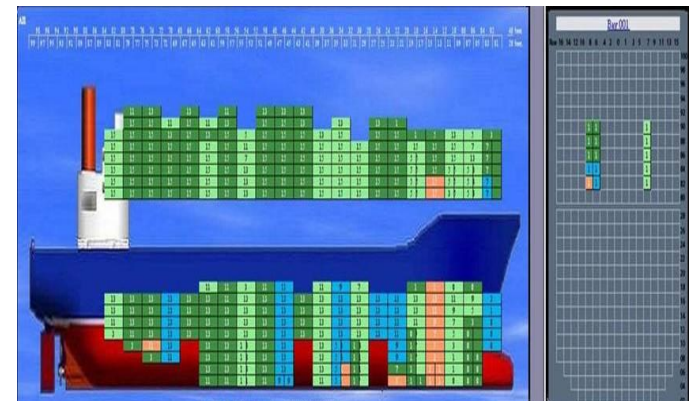
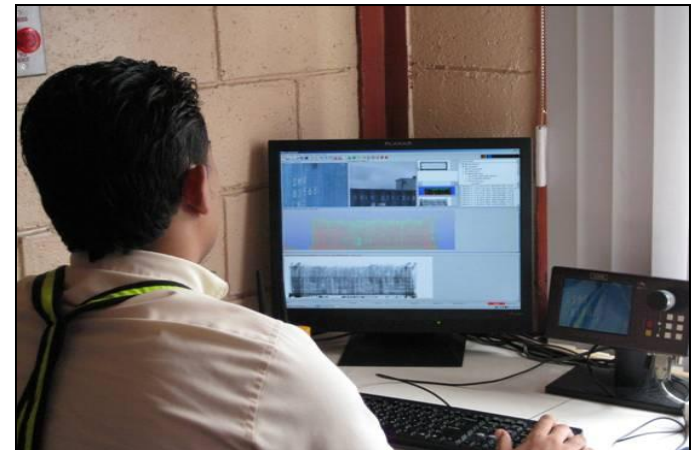
SUPPLY CHAIN SECURITY

Screening & Targeting Containers

Cargo screening and inspections

- 24 Hour Rule
 - Requires submission of complete and accurate manifest information 24 hours before a container is loaded onto a U.S.-bound vessel
- Automated Targeting System (ATS)
 - Computerized model to help to identify potentially high-risk containers for inspection
- Importer Security Filing and Additional Carrier Requirements /10+2 Rule
 - Requires additional information from importers and vessel stow plans to identify incorrectly manifested containers
- GAO has reported that CBP has made progress incorporating the new 10+2 Rule, but has generally not conducted timely evaluations of ATS effectiveness or improvements

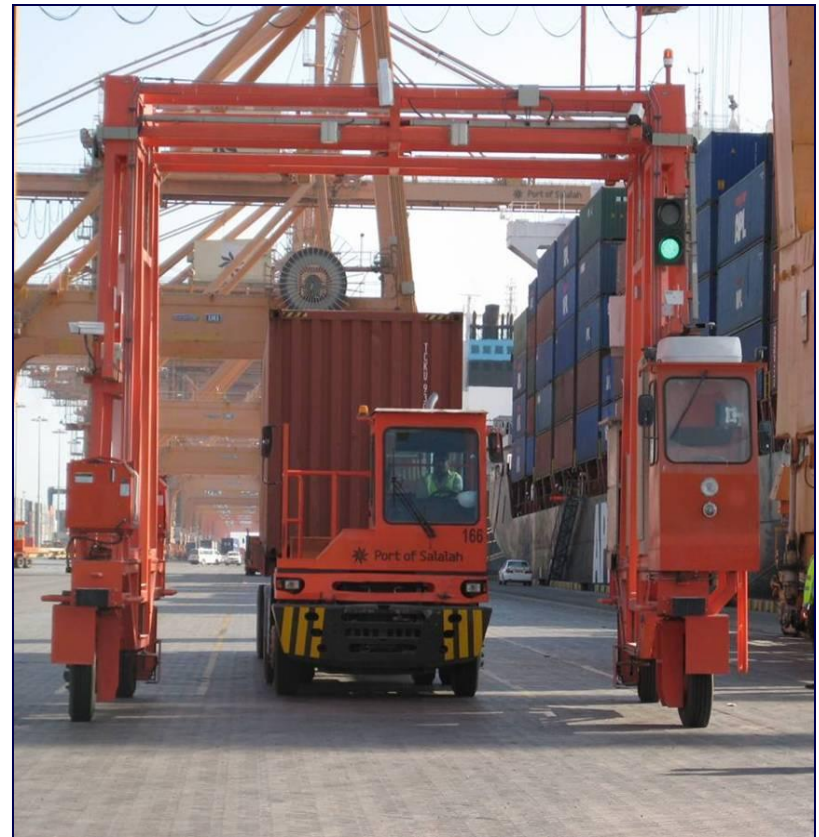
Reference: GAO-04-557T, GAO-10-841, GAO-13-9



SUPPLY CHAIN SECURITY

Deploying New Technologies

- Technologies deployed to scan containers for nuclear materials and other contraband
 - CBP and DNDI have deployed over 1,400 radiation portal monitors in U.S.
 - Radiation monitors installed in primary inspection lanes to inspect nearly all traffic and containers
 - CBP conducts further inspections at secondary location, if monitor alarms
 - Pilots, like Secure Freight Initiative, used as test bed for technologies (e.g., MRDIS for use on quays)
 - However, some technologies (ASP and CAARS) were rushed into acquisition without appropriate operational tests
 - References GAO-12-941T, GAO-10-1041T



SUPPLY CHAIN SECURITY

Industry Partnerships

Partnering with the trade industry

- Customs-Trade Partnership Against Terrorism (C-TPAT) voluntary program between CBP and private companies
 - CBP reviews security of private company international supply chain to improve security of U.S.-bound shipments
 - Private companies benefit from reduced inspections and lower cargo shipment wait times
- CBP had accepted or initially certified over 10,000 companies
- GAO work on C-TPAT showed
 - Program provides CBP with information otherwise not available
 - Program positions CBP to identify changes that could improve supply chain security
 - CBP has strengthened program management

References: GAO-08-240, GAO-10-12, GAO-12-422T



SUPPLY CHAIN SECURITY

Bilateral Cooperation via Container Security Initiative

Container Security Initiative (CSI)

- Bilateral government partnership program that stations CBP officers in foreign seaports
- CBP officers work with host customs officials to identify and examine high risk U.S.-bound containers
- CBP had staff at 58 foreign seaports, accounting for 86 percent of U.S. bound shipments
- GAO work on CSI showed
 - Program has met strategic goals in terms of CSI locations and proportion of U.S.-bound shipments
 - Improved relationships with host governments through increased information sharing
 - CBP decreased CSI operating cost by \$35 million by doing some of the targeting remotely
 - New GAO review underway looking at CSI

References: GAO-05-557, GAO-08-187, GAO-12-422T



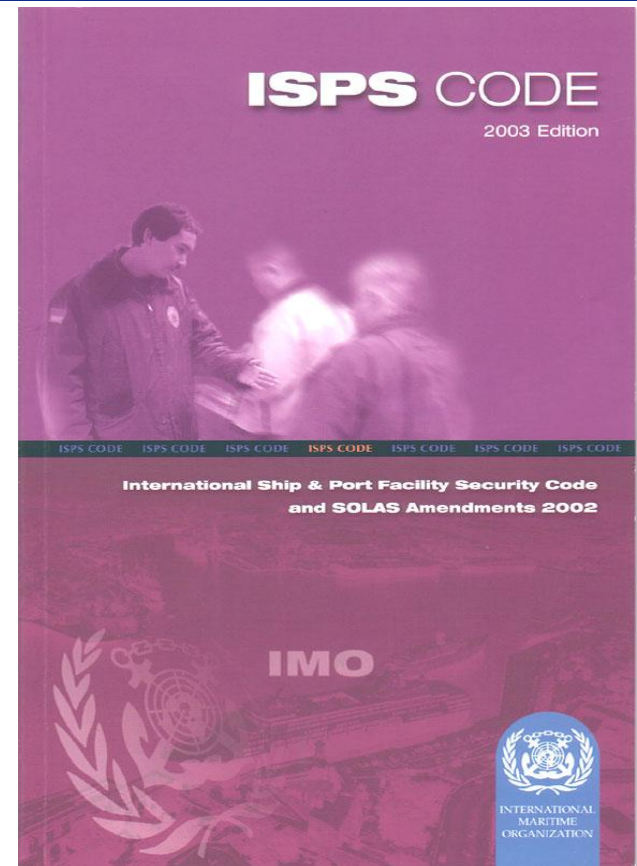
SUPPLY CHAIN SECURITY

International Port Security Program

International Port Security (IPS) program

- As required by MTSA and SAFE Port Act Coast Guard reviews security measures at foreign ports against international standards (the IMO's International Ship and Port Facility Security Code, AKA the ISPS Code)
- GAO work on the IPS program showed that the Coast Guard
 - Had visited and assessed over 100 countries
 - Implemented a risk-based approach to plan visits and focus resources
 - Improved relationships and security at foreign ports despite sovereignty concerns and lack of resources

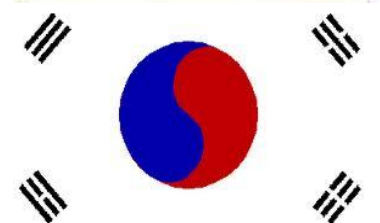
References: GAO-08-126T, GAO-10-940T



SUPPLY CHAIN SECURITY

Mutual Recognition Arrangements (MRA)

- MRAs recognizes security practices between nations to enhance the efficiency and security of shipments throughout the global supply chain
 - CBP MRAs compliment C-TPAT by allowing supply chain security-related practices and programs taken by one country to be recognized by another. As of March 2013, CBP has signed seven MRAs.
 - Coast Guard MRA with European Union recognizes the various countries' port security regimes and inspection results.
 - Reference: GAO-08-538, GAO-10-940T, GAO-12-1009T



ENDURING CHALLENGES

Program Management and Implementation

Lack of planning

- Rush to respond to events, such as 9/11, resulted in “implement and amend” approach that negatively affected management of some programs
 - CBP rolled out CSI without a strategic plan or work force plan
 - Initial implementation of C-TPAT lacked a human capital plan

Lack of adequate internal controls

- Several maritime security programs lacked adequate internal controls
 - GAO found that the Coast Guard lacked procedures to ensure field units inspected offshore energy facilities annually, in accordance with its guidance
 - GAO investigators were able to successfully access secure port areas with counterfeit TWIC credentials

Inadequate acquisition management

- Some acquisition programs experienced planning and development challenges
 - DHS cancelled DNDO’s advanced spectroscopic portal (ASP) program after the radiation detection monitors did not test well enough to deploy – approximate cost \$280 million
 - DHS cancelled DNDO’s acquisition and deployment phase of a cargo radiography system since the machines did not meet existing requirements – approximate cost \$113 million

ENDURING CHALLENGES

Partnerships and Collaboration

Lack of port partner coordination

- Challenges remain stemming from issues related to launching programs without adequate stakeholder coordination
 - Coast Guard launched IOCSs and information sharing program, WatchKeeper, without input from key law enforcement agencies and port partners, and partners did not log into the system

Challenges coordinating with multiple levels of stakeholders

- Other federal agencies
 - Lack of interagency collaboration and defined roles in some of the key planning documents / strategies
- Private sector stakeholders
 - Lack of information sharing between cruise lines and CBP has challenged efforts to increase port security by screening cruise line passengers
- International stakeholders
 - Sovereignty concerns have limited the Coast Guard's ability to assess foreign port security under IPS program & CBP's ability to station staff in foreign ports for CSI



ENDURING CHALLENGES

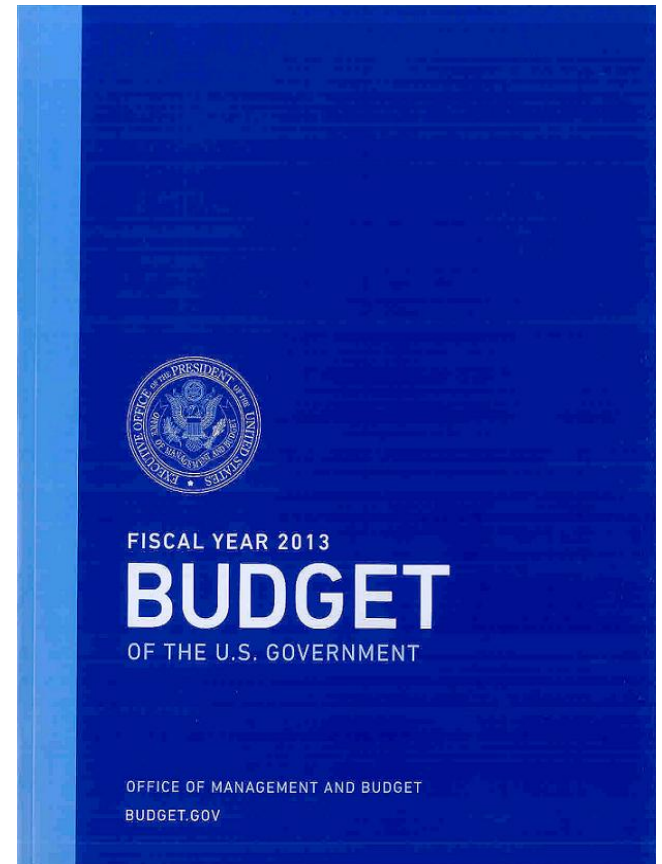
Resources, Funding, and Sustainability

Human capital shortfalls

- Limited personnel and staffing time and rotations continue to pose a challenge to maritime security
 - GAO has reported that limited staff time has challenged the Coast Guard's ability to incorporate MSRAM into strategic, operational, and tactical planning, as well as meet inspection requirements

Budget, sequester and funding constraints

- Budget constraints have required DHS to prioritize
 - Some Coast Guard units are unable to meet self-imposed standards for some activities, such as boarding and escorting vessels
 - Decrease in technical assistance for IPSP has required the Coast Guard to partner with other federal agencies and international organizations to secure funding for foreign port security improvement projects



ENDURING CHALLENGES

Performance Measures

Lack of reliable and accurate data

- Challenges collecting complete, accurate, and reliable data
 - Variance in illegal seafarer data collected by CBP and Coast Guard was unreliable for informing strategic and tactical plans
 - Flaws in the Maritime Information for Safety & Law Enforcement database (MISLE) limited the Coast Guard's ability to assess inspection activities

Not using data to manage programs

- DHS and component agencies have not always had or used performance information to manage their missions
 - Coast Guard used MISLE to review facility inspection results, but did not use the data to evaluate the facility inspection program overall

Lack of outcome-based performance measures

- Difficulties developing and using performance measures that focus on outcomes, i.e. the intended result of carrying out a program or activity
 - C-TPAT performance measures focused on participation and facilitating trade, not on improving supply chain security
 - Coast Guard faced challenges using its performance measure for reducing maritime risk to inform decisions

CONCLUSIONS ON MTSA

After 10 Years...

- DHS and its component agencies have made substantial progress in implementing various programs that, collectively, have improved maritime security
- Agencies also encountered challenges in implementing these programs
 - Some of the reasons were based on weak management of programs
 - Some of the reasons were based on inherent nature of the maritime domain and its characteristics

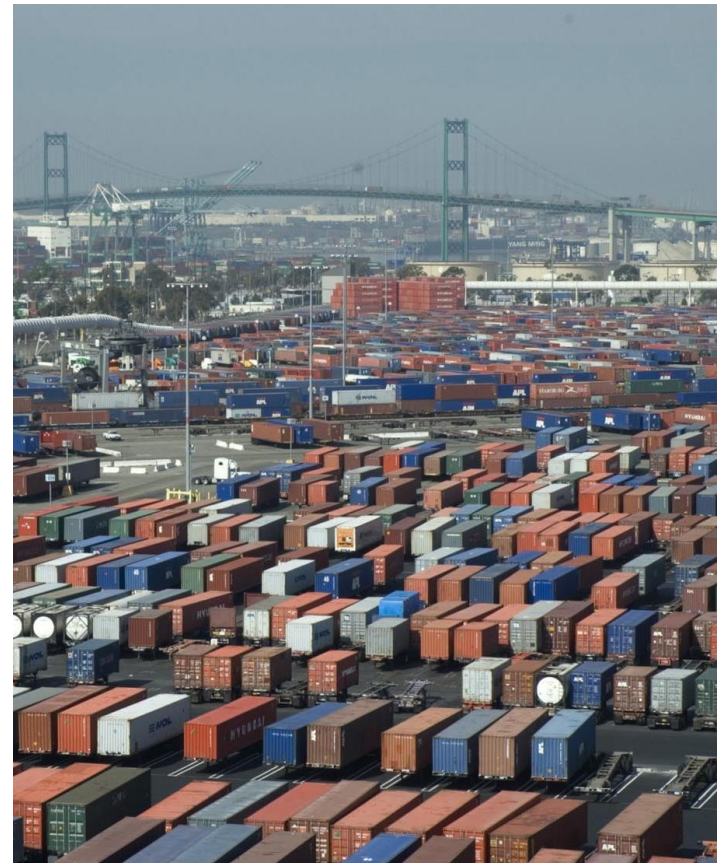


ONGOING ENGAGEMENTS

Global Supply Chain Security Strategy

GAO objectives:

- To what extent has DHS assessed or re-assessed the foreign ports that pose the greatest risk to the global supply chain and focused its maritime programs to address risks from those ports?
- What actions has DHS taken to improve the efficiency and effectiveness of its maritime supply chain security programs?
- NOTE: GAO will mainly focus on Coast Guard and CBP programs, such as ISPS, CSI, CTPAT and MRAs

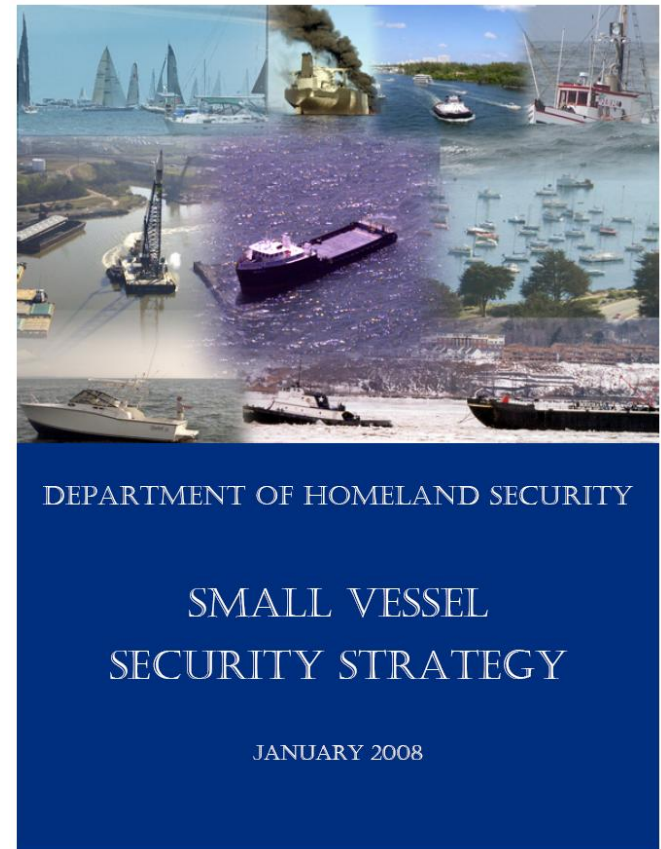


ONGOING ENGAGEMENTS

Small Vessel Security Strategy

GAO Objective:

- To what extent have DHS and its components made and tracked progress in addressing action items in the Small Vessel Security Strategy Implementation Plan?
- NOTE: The strategy was issued in January 2008, and the Implementation Plan was issued in January 2011. GAO work will focus on Coast Guard, CBP, DNDO, and S&T, and visit 2 ports



ONGOING ENGAGEMENTS

Cruise Ship Security and Safety

GAO Objectives:

- What is the nature and extent of security and safety incidents for cruise ships visiting U.S. ports 2008-2011?
- To what extent have the cruise ship industry and federal agencies taken actions to implement the Cruise Vessel Security and Safety Act?
- To what extent have federal agencies and the cruise ship industry taken other actions to enhance safety [since the Costa Concordia accident] and what challenges, have they encountered?

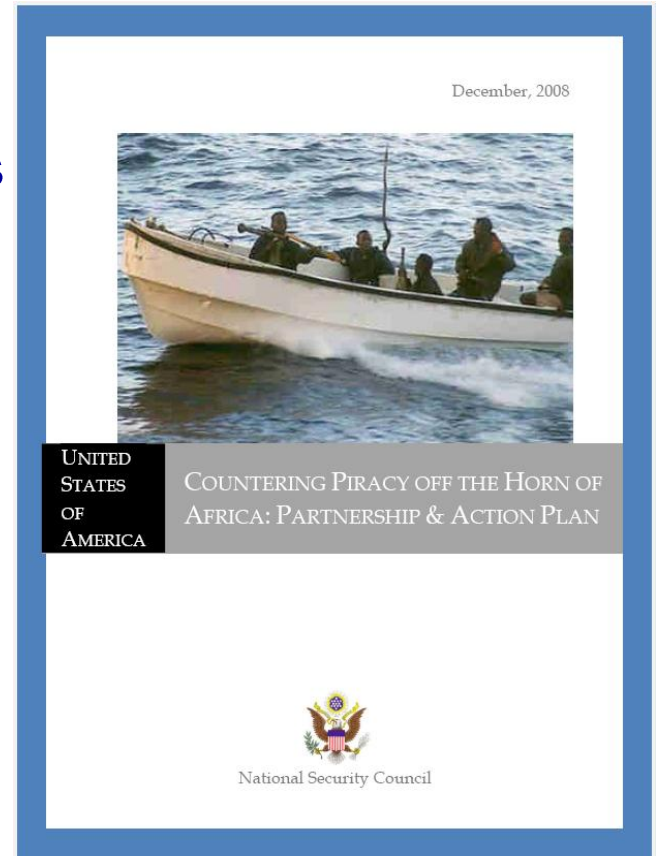


ONGOING ENGAGEMENTS

Update on Maritime Piracy

GAO Objectives:

- To what extent have counter-piracy plans, practices, and collaboration efforts helped in preventing or disrupting incidents of piracy off the Horn of Africa?
- How does the US Government track information on ransom payments and pirate financing and to what extent is this information used in the disruption and prosecution of pirate networks?
- Can similar efforts be used to inform an approach to counter piracy in the Gulf of Guinea?

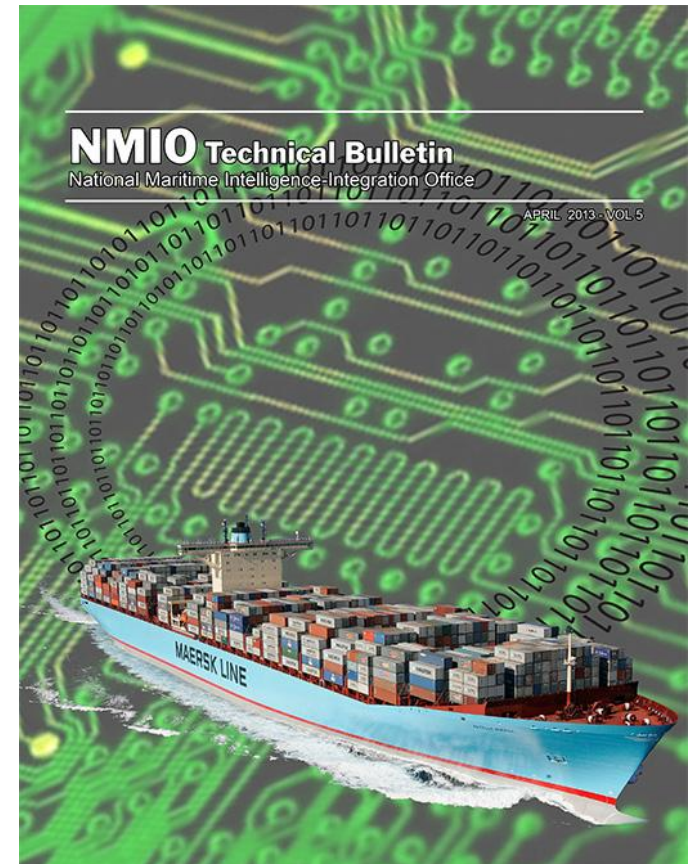


ONGOING ENGAGEMENTS

Maritime Cybersecurity

GAO Objectives:

- To what extent do cybersecurity threats exist within the maritime environment?
- To what extent do current laws and regulations recognize and address such cybersecurity threats?
- To what extent do DHS and other federal and nonfederal stakeholders have taken steps to identify and mitigate maritime-related cyber threats?
- NOTE: GAO is current making decisions on scope, ports to visit, whether to include vessels and whether to include government IT systems



ONGOING ENGAGEMENTS

Maritime Cybersecurity

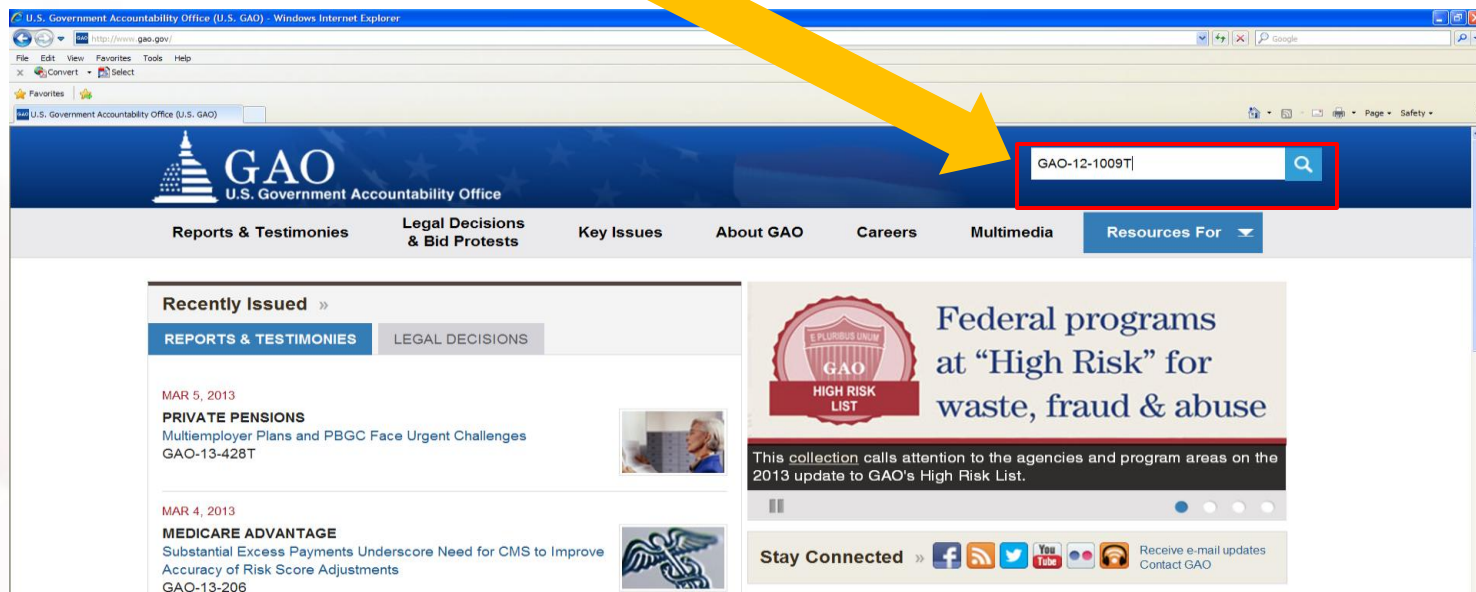
- GAO is looking to obtain input from a broad range of representatives within the domestic and international maritime industry on current state of cybersecurity
- GAO can keep sources anonymous by not naming them (i.e., specific ports or industry groups) in its public reports
- GAO is seeking industry perspectives on:
 - Systems/information technology that are critical to port operations;
 - Cyber-related threats and vulnerabilities facing port and facility operators;
 - Maritime industry efforts to incorporate cybersecurity into its risk management practices; and
 - Federal efforts to enhance cybersecurity in the maritime sector

QUESTIONS AND GAO CONTACT

Questions?

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

GAO website: www.gao.gov



The screenshot shows the GAO website homepage in a Windows Internet Explorer browser window. The address bar displays "http://www.gao.gov". The page features a blue header with the GAO logo and the text "U.S. Government Accountability Office". Below the header is a navigation menu with links for "Reports & Testimonies", "Legal Decisions & Bid Protests", "Key Issues", "About GAO", "Careers", "Multimedia", and "Resources For". A search bar is located in the top right corner of the page, containing the text "GAO-12-1009T" and a magnifying glass icon. A red box highlights the search bar, and a yellow arrow points from the text "GAO website: www.gao.gov" to the search bar. The main content area includes a "Recently Issued" section with two entries: "PRIVATE PENSIONS" dated MAR 5, 2013, and "MEDICARE ADVANTAGE" dated MAR 4, 2013. There is also a "Federal programs at 'High Risk' for waste, fraud & abuse" section with a "HIGH RISK LIST" badge. At the bottom, there is a "Stay Connected" section with social media icons for Facebook, RSS, Twitter, YouTube, and LinkedIn, and a link to "Receive e-mail updates Contact GAO".

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.

