Comparing Results of Maritime Cybersecurity Studies from Selected Countries

Stephen L. Caldwell

Former Director, Maritime and Supply Chain Security Issues

at the U.S. Government Accountability Office

CCICADA Maritime Cybersecurity Conference

Rutgers University, NJ / March 2-3, 2015

AGENDA

- Background
- Cyber Systems
- Cyber Threats
- Cyber Studies
- Comparing Studies
- Questions & Contact Info

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

G A O

Accountability * Integrity * Reliability

GAO-04-838

BACKGROUND

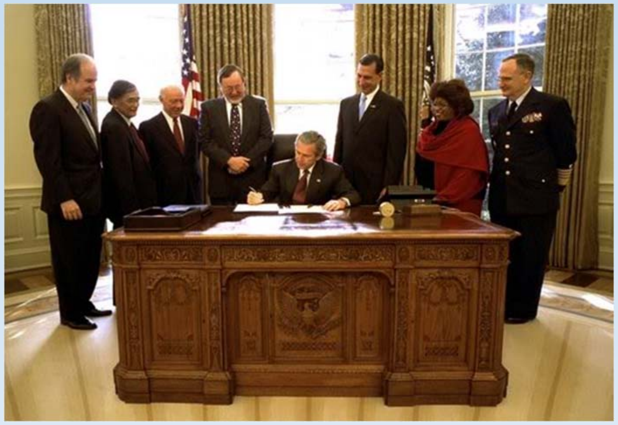
U.S. Government Accountability Office (GAO)

- 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 about 100 reports on maritime and supply chain security
- Stephen L. Caldwell was the director in charge of the maritime and supply chain security portfolio from 2006-2015

BACKGROUND

Legislation and Directives

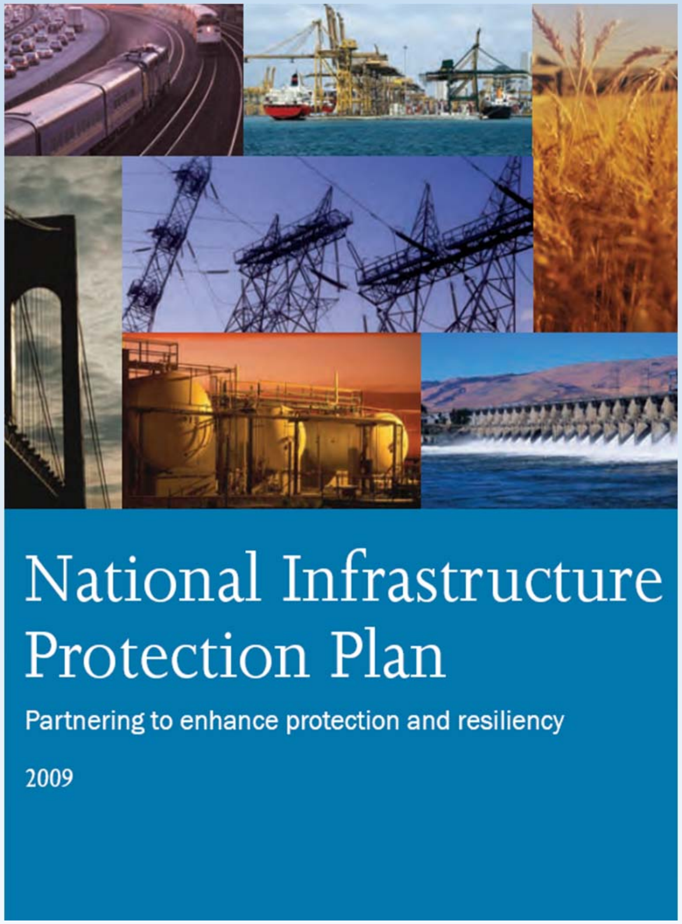
- The Maritime Transportation Security Act (MTSA) of 2002, passed to protect the nation's ports and waterways by requiring a wide range of security improvements, many by U.S. Coast Guard (USCG) and industry
- Presidential Policy Directive (PDD) 21, sets forth a unified strategy to address the all-hazards risks posed to critical infrastructure
- The National Infrastructure Protection Plan (NIPP) set up a framework to address cyber risks, information sharing, and development of sector plans
- Executive Order (EO) 13636 requires enhanced information sharing with the cyber private sector, prioritization of cyber security actions, and identification of cyber risks



CYBER SYSTEMS

Importance of Cyber Systems

- The NIPP, PPD, and EO place increasing emphasis on addressing both physical and cyber protection of infrastructure in an integrated fashion
- Maritime critical infrastructure has become increasingly interconnected with and dependent on cyber systems
- The operations of ports are supported by information and communication systems, such as
  - Terminal Operating Systems (slide 6)
  - Business Operations Systems (slide 6)
  - Industrial Control Systems (slide 7)
  - Access Control and Monitoring Systems (slide 8)



National Infrastructure Protection Plan

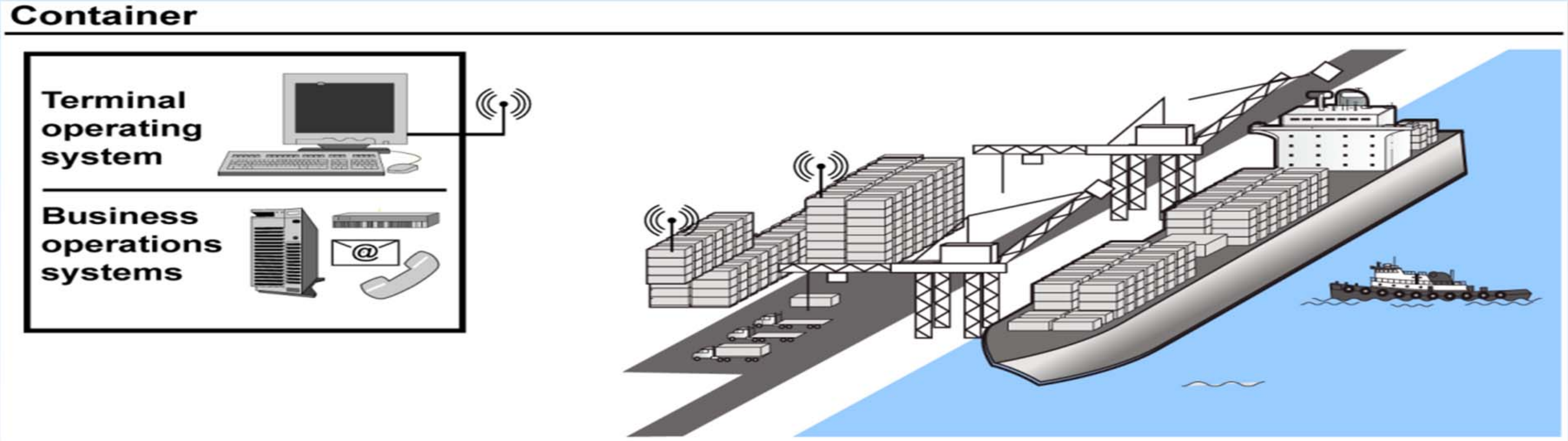
Partnering to enhance protection and resiliency

2009

CYBER SYSTEMS

Terminal and Business Operating Systems

- Terminal operating systems are information systems used by terminal operators to control container movements and storage
- Business operation systems are information and communications technologies used to help support the business operations of the terminal, such as communicating with customers and preparing invoices

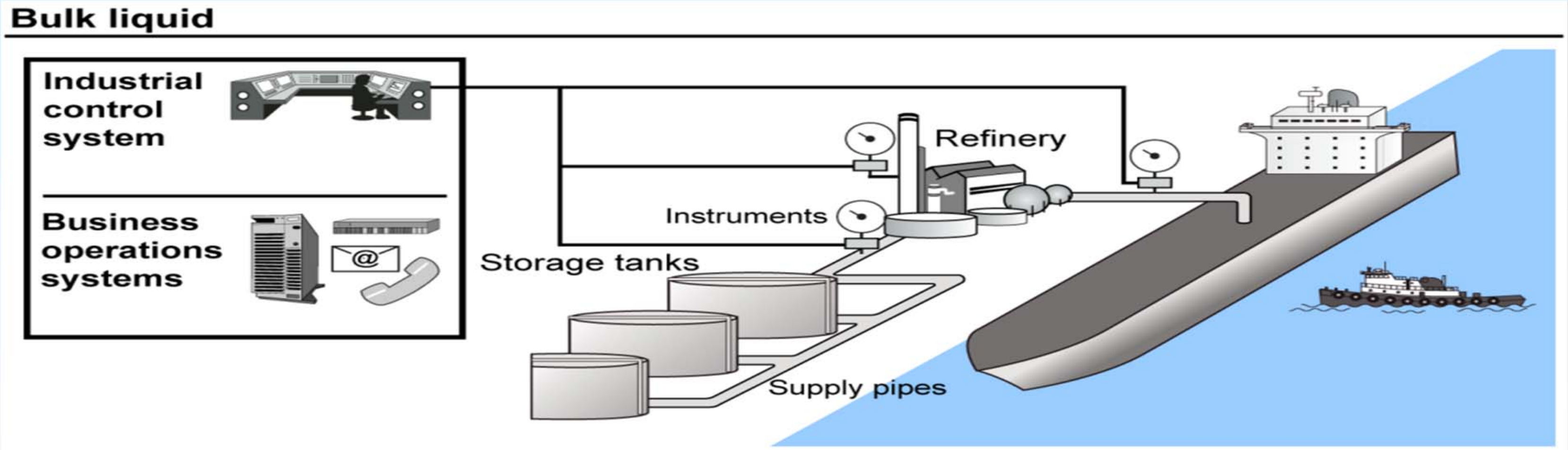


Source: GAO analysis of maritime sector information; Art Explosion (clip art).

CYBER SYSTEMS

Industrial Control Systems

- Industrial control systems are automated systems used to control industrial processes such as manufacturing, product handling, production and distribution
- These systems are used to operate motors, pumps, valves, signals, lighting, and access controls, and to facilitate the movement of goods throughout maritime terminals using conveyor belts or pipelines

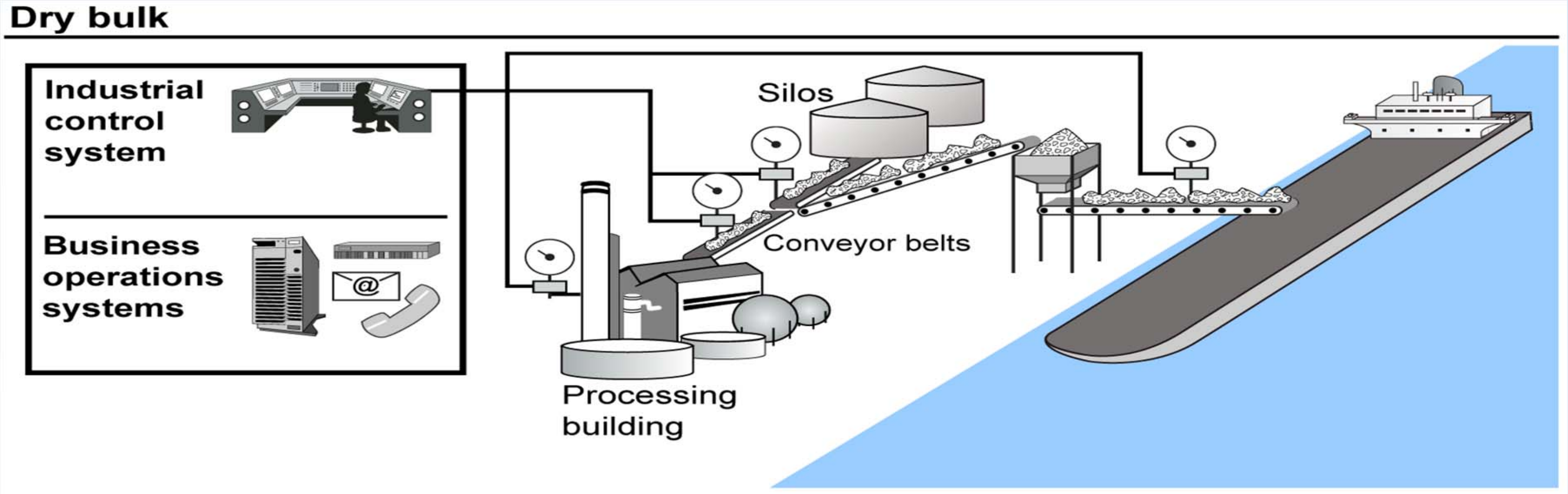


Source: GAO analysis of maritime sector information; Art Explosion (clip art).

CYBER SYSTEMS

Access Control and Monitoring Systems

- Access control and monitoring systems are information and communication technologies that support physical security operations
- These systems include camera surveillance systems that can be connected to information system networks to facilitate remote monitoring of port facilities, and electronically enabled physical access control devices



Source: GAO analysis of maritime sector information; Art Explosion (clip art).

CYBER THREATS

Cyber Threat Actors

- Threats come from a wide array of sources:
  - Bot-network operators
  - Business competitors
  - Criminal groups
  - Hackers
  - Insiders
  - Foreign Nations
  - Phishers
  - Spammers
  - Spyware or malware authors
  - Terrorists

CYBER THREATS

Cyber Threat Types

- These types of cyber threats may adversely affect information and communications networks:
  - Denial of service
  - Distributed denial of service
  - Phishing
  - Trojan Horse
  - Virus
  - Worm
  - Exploits affecting the information technology chain
- For expanded view of this graphic, see GAO-07-705, p.6

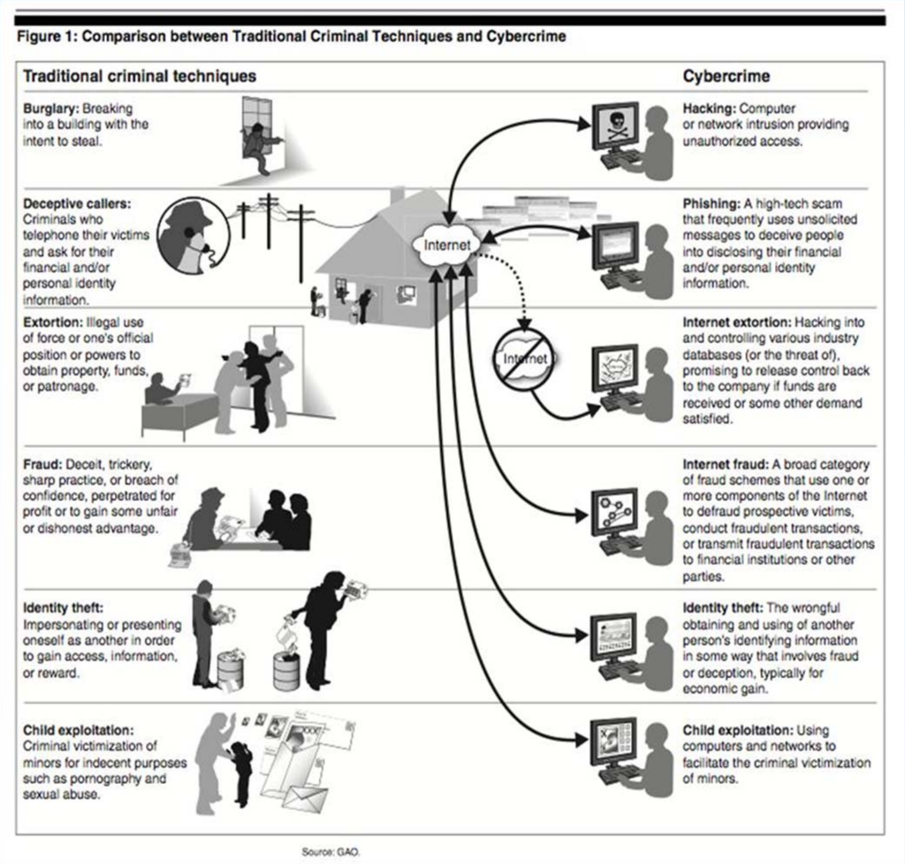


Figure 1: Comparison between Traditional Criminal Techniques and Cybercrime

Traditional criminal techniques

Burglary: Breaking into a building with the intent to steal.

Deceptive callers: Criminals who telephone their victims and ask for their financial and/or personal identity information.

Extortion: Illegal use of force or one's official position or powers to obtain property, funds, or patronage.

Fraud: Deceit, trickery, sharp practice, or breach of confidence, perpetrated for profit or to gain some unfair or dishonest advantage.

Identity theft: Impersonating or presenting oneself as another in order to gain access, information, or reward.

Child exploitation: Criminal victimization of minors for indecent purposes such as pornography and sexual abuse.

Cybercrime

Hacking: Computer or network intrusion providing unauthorized access.

Phishing: A high-tech scam that frequently uses unsolicited messages to deceive people into disclosing their financial and/or personal identity information.

Internet extortion: Hacking into and controlling various industry databases (or the threat of), promising to release control back to the company if funds are received or some other demand satisfied.

Internet fraud: A broad category of fraud schemes that use one or more components of the Internet to defraud prospective victims, conduct fraudulent transactions, or transmit fraudulent transactions to financial institutions or other parties.

Identity theft: The wrongful obtaining and using of another person's identifying information in some way that involves fraud or deception, typically for economic gain.

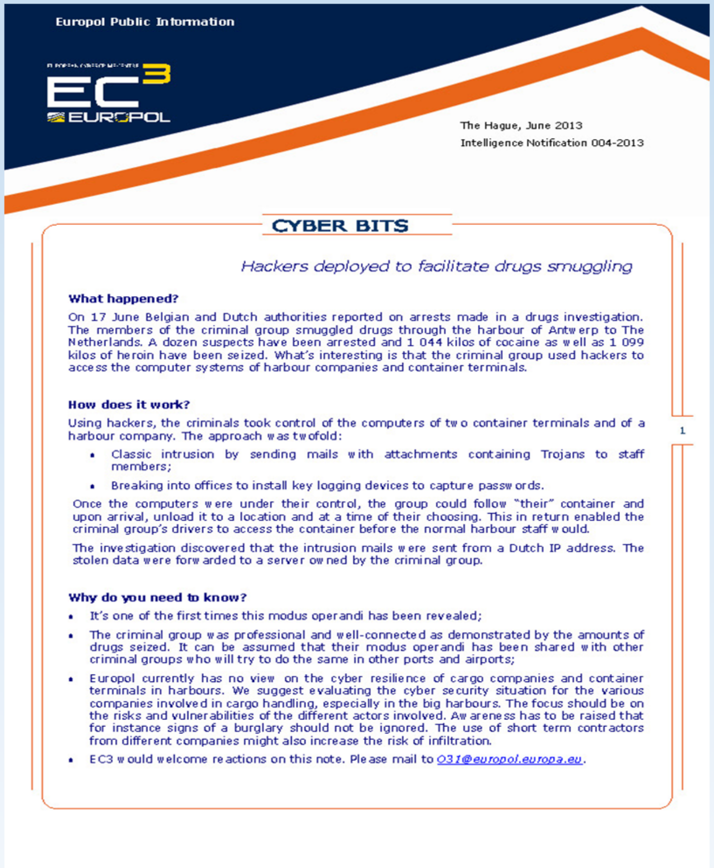
Child exploitation: Using computers and networks to facilitate the criminal victimization of minors.

Source: GAO.

CYBER THREATS

Port Cybersecurity Incident in Europe

- In June 2013, Belgian and Dutch authorities reported that drug smugglers had employed professional hackers to conduct criminal operations
- The criminal group successfully smuggled 1,044 kilos of cocaine and 1,099 kilos of heroin through the port of Antwerp on to the Netherlands
- The hackers emailed trojan horses and installed key stroke logging devices to capture passwords, allowing them to gain control of the port computers and terminal operating system
- The criminals were then able to monitor “their” container, and unload it at a time and location of their choosing, avoiding normal port staff



Europol Public Information

EC3
EUROPOL

The Hague, June 2013
Intelligence Notification 004-2013

CYBER BITS

Hackers deployed to facilitate drugs smuggling

What happened?

On 17 June Belgian and Dutch authorities reported on arrests made in a drugs investigation. The members of the criminal group smuggled drugs through the harbour of Antwerp to The Netherlands. A dozen suspects have been arrested and 1 044 kilos of cocaine as well as 1 099 kilos of heroin have been seized. What’s interesting is that the criminal group used hackers to access the computer systems of harbour companies and container terminals.

How does it work?

Using hackers, the criminals took control of the computers of two container terminals and of a harbour company. The approach was twofold:

- Classic intrusion by sending mails with attachments containing Trojans to staff members;
- Breaking into offices to install key logging devices to capture passwords.

Once the computers were under their control, the group could follow “their” container and upon arrival, unload it to a location and at a time of their choosing. This in return enabled the criminal group’s drivers to access the container before the normal harbour staff would.

The investigation discovered that the intrusion mails were sent from a Dutch IP address. The stolen data were forwarded to a server owned by the criminal group.

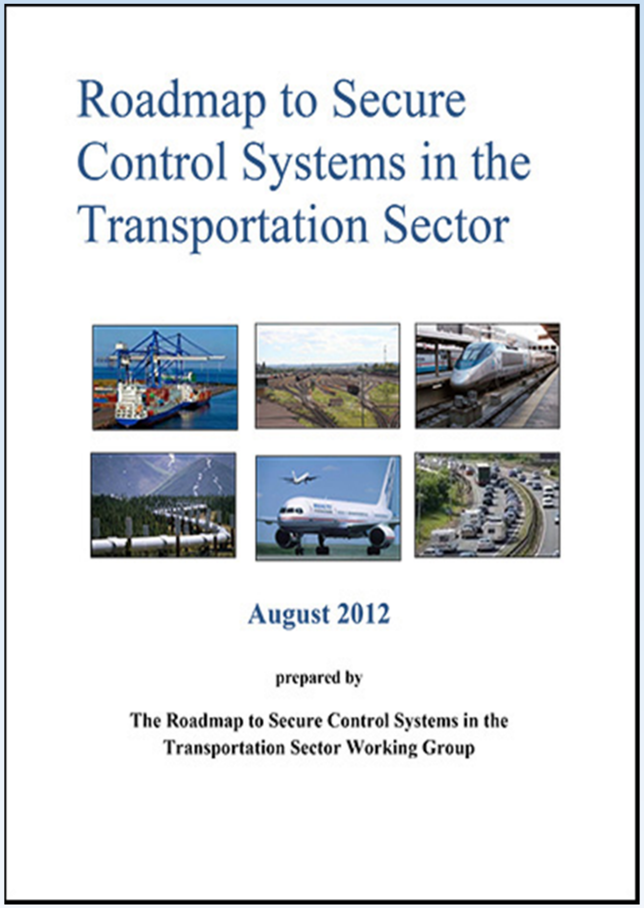
Why do you need to know?

- It’s one of the first times this modus operandi has been revealed;
- The criminal group was professional and well-connected as demonstrated by the amounts of drugs seized. It can be assumed that their modus operandi has been shared with other criminal groups who will try to do the same in other ports and airports;
- Europol currently has no view on the cyber resilience of cargo companies and container terminals in harbours. We suggest evaluating the cyber security situation for the various companies involved in cargo handling, especially in the big harbours. The focus should be on the risks and vulnerabilities of the different actors involved. Awareness has to be raised that for instance signs of a burglary should not be ignored. The use of short term contractors from different companies might also increase the risk of infiltration.
- EC3 would welcome reactions on this note. Please mail to O31@europol.europa.eu.

CYBER STUDIES

U.S. TSWG Roadmap to Secure Control Systems

- Title: *Roadmap to Secure Control Systems in the Transportation Sector*, Aug. 2012
- By the Transportation Sector Working Group (TSWG), created by DHS, National Cybersecurity Division, Control Systems Security Program
- Approach: government and industry experts developed goals, objectives, metrics and milestones to measure cybersecurity posture in the transportation sector over 10 years
- Scope: limited to all U.S. transportation modes, therefore few specifics on maritime (which are generally descriptive of that mode)
- Recommendations: to implement the roadmap through buy-in, action plans, prioritize actions, and communicate results



Roadmap to Secure Control Systems in the Transportation Sector

August 2012

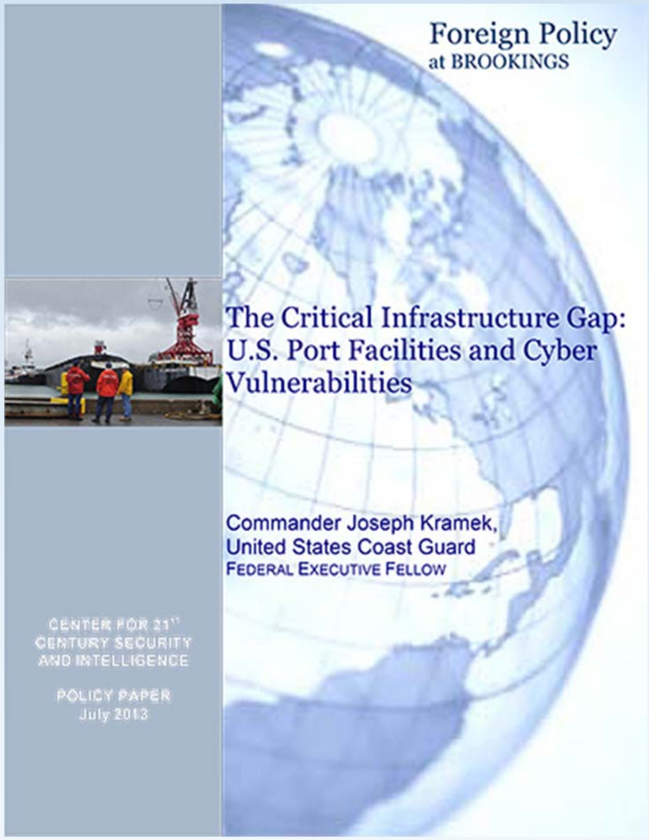
prepared by

The Roadmap to Secure Control Systems in the Transportation Sector Working Group

CYBER STUDIES

Brookings Institute Policy Paper

- Title: *The Critical Infrastructure Gap: U.S. Port Facilities and Cyber Vulnerabilities*, July 2013
- By the Brookings Institution, Center for 21st Century Security and Intelligence
- Approach: case studies using interviews with variety of stakeholders, analysis of grant programs and funding, and literature review
- Scope: included 6 diverse ports in U.S., focusing on port facilities; not vessels
- Recommendations: to Congress, DHS, USCG, FEMA and industry re: assessing requirements and resources, determining vulnerabilities, and developing response plans



Foreign Policy
at BROOKINGS

The Critical Infrastructure Gap:
U.S. Port Facilities and Cyber
Vulnerabilities

Commander Joseph Kramek,
United States Coast Guard
FEDERAL EXECUTIVE FELLOW

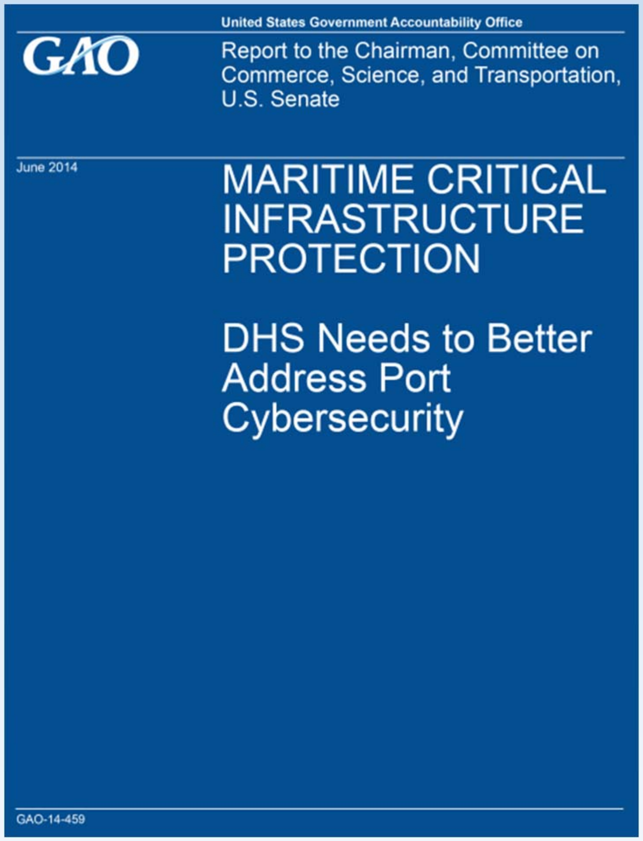
CENTER FOR 21ST
CENTURY SECURITY
AND INTELLIGENCE

POLICY PAPER
July 2013

CYBER STUDIES

U.S. GAO Report GAO-14-459

- Title: *Maritime Critical Infrastructure Protection: DHS Needs to Better Address Cybersecurity*, June 2014
- Joint by GAO's Information Technology and Homeland Security and Justice Teams
- Approach: used MTSA, PDD, EO and NIPP as criteria to assess DHS progress
- Scope: port facilities covered by the U.S. MTSA statute; also included Port Security Grant Program; did not include vessels
- Recommendations: to USCG and FEMA regarding risk assessments, threat information sharing, and expertise used to assess grants



United States Government Accountability Office

GAO

Report to the Chairman, Committee on Commerce, Science, and Transportation, U.S. Senate

June 2014

MARITIME CRITICAL INFRASTRUCTURE PROTECTION

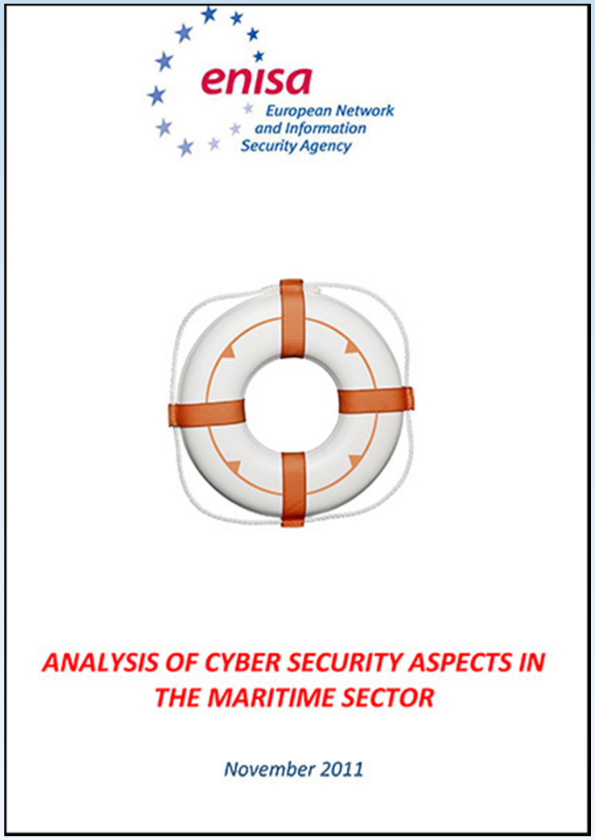
DHS Needs to Better Address Port Cybersecurity

GAO-14-459

CYBER STUDIES

European ENISA Analysis

- Title: *Analysis of Cyber Security Aspects in the Maritime Sector*, Nov. 2011
- By the European Network and Information Security Agency (ENISA)
- Approach: conducted desk research of literature, review of regulations, conducted interviews and questionaires, and held a validation workshop
- Scope: the maritime sector in Europe, such as port facilities (and possibly vessels), with some review of international governance issues
- Recommendations: to raise awareness, develop strategies, define roles and responsibilities, develop standards, conduct training, consider regulations, harmonize international & EU actions



enisa

European Network and Information Security Agency

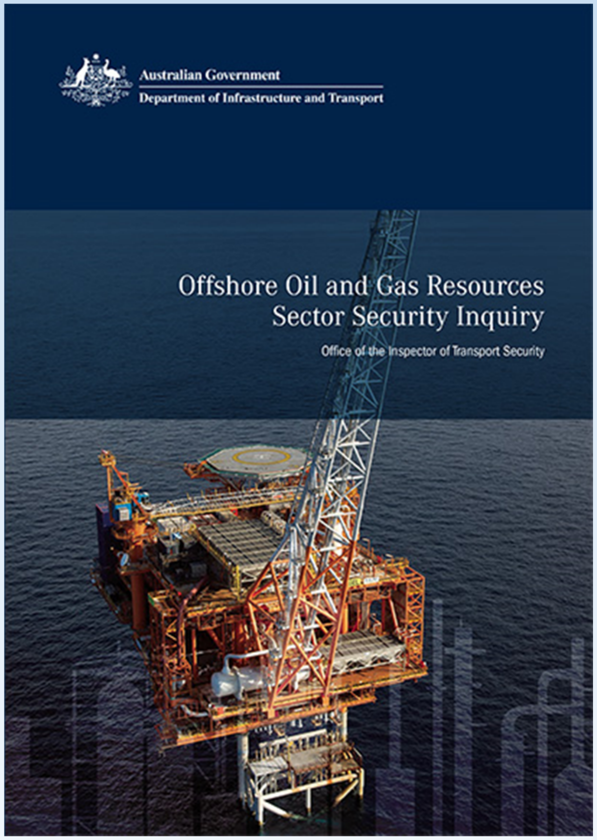
ANALYSIS OF CYBER SECURITY ASPECTS IN THE MARITIME SECTOR

November 2011

CYBER STUDIES

Australian OITS Government Inquiry

- Title: *Offshore Oil and Gas Resources Sector Security Inquiry*, June 2012 (pages 107-110)
- By Dept. of Infrastructure and Transport, Office of the Inspector of Transport Security (OITS)
- Approach: review of international and Australia legal and regulatory regimes, interviews with government and industry, including site visits to offshore facilities (and U.S., U.K., and Norway)
- Scope: examined Australia's maritime oil and gas sector (focusing on offshore infrastructure); cyber was only one of many components examined
- Recommendations: (re: cyber) training at both the executive and operational level, conduct exercises, and examine other improvements



Australian Government
Department of Infrastructure and Transport

Offshore Oil and Gas Resources
Sector Security Inquiry
Office of the Inspector of Transport Security

COMPARING STUDIES

Making Comparisons and Common Themes

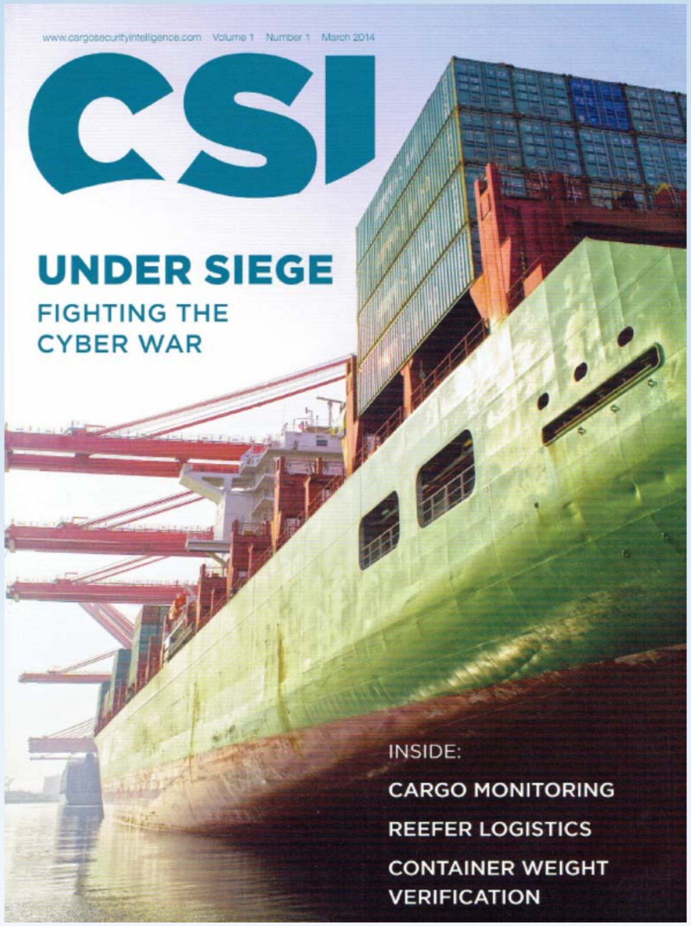
- It is difficult to make direct comparisons due to differences in the studies' purpose, scope, methodology and organization
- However, they have common themes that reinforce areas of concern and needed action:
    - Maritime operations are growing more automated and interconnected
    - Stakeholder awareness of cyber threats and their cyber hygiene has been weak
    - Vulnerabilities exist, with potentially harmful consequences to ports
    - Risk assessments to date have generally focused on physical (not cyber) security
    - Threat information sharing is ad hoc and needs to be improved

NAVY / MARINE CORPS / COAST GUARD / MERCHANT MARINE
SEAPOWER
THE NEXT PLAYGROUND FOR HACKERS?
November 2014 $5.00
NAVY LEAGUE OF THE UNITED STATES
www.navyleague.org
NAVY LEAGUE
AMERICA JOINS THE FLEET / SPECIAL REPORT: MAINTENANCE, REPAIR & OVERHAUL

COMPARING STUDIES

Maritime Environment

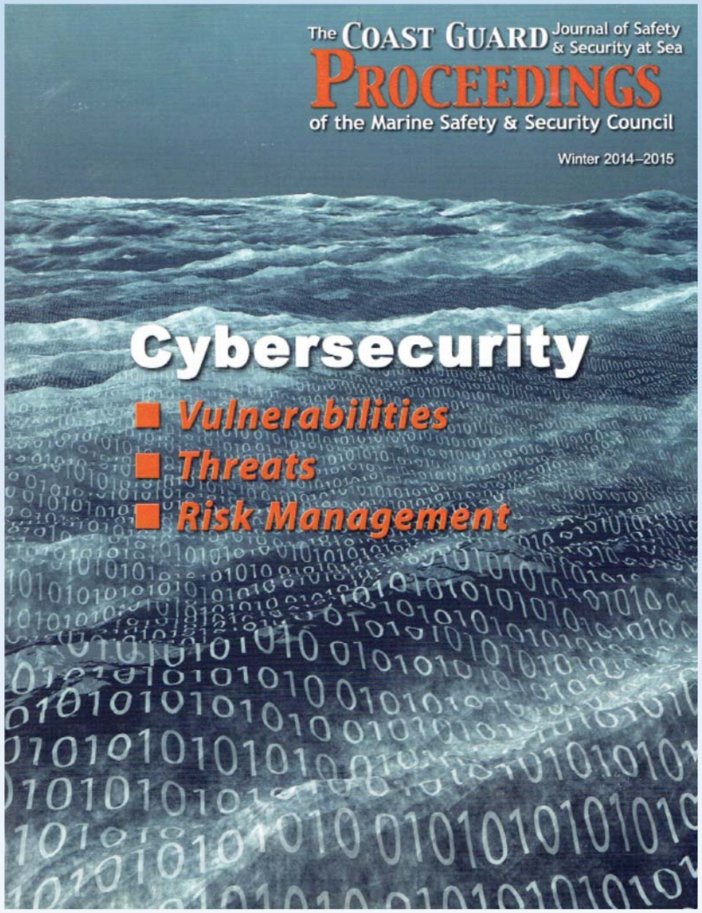
- Maritime operations are growing more automated and interconnected
  - Complex networked logistics management systems undergird the global flow of maritime commerce (Brookings)
  - Maritime activity increasingly relies on info communications and technology to optimize navigation, propulsion, and traffic control (ENISA)
  - SCADA systems are used to control all operational aspects, including remote operations, of ship-to-shore and rail-mounted gantry cranes, at marine ports and terminals (TSWG)
  - Current maritime governance is fragmented among various stakeholders (ENISA)


www.cargosecurityintelligence.com Volume 1 Number 1 March 2014
CSI
UNDER SIEGE
FIGHTING THE CYBER WAR
INSIDE:
CARGO MONITORING
REEFER LOGISTICS
CONTAINER WEIGHT VERIFICATION

COMPARING STUDIES

Awareness and Hygiene

- Stakeholder awareness of cyber threats and their cyber hygiene has been weak
  - The level of cybersecurity awareness and culture in U.S. maritime facilities is relatively low (Brookings)
  - Cybersecurity awareness in the maritime sector is low to non-existent (ENISA)
  - Cyber support services are contracted out without consideration of the security of foreign owned contractors (TSWG)
  - FEMA has not consulted cybersecurity SMEs to inform the review of cyber-related grant proposals (GAO)
  - Basic cybersecurity hygiene is not being practiced (Brookings)


The COAST GUARD Journal of Safety & Security at Sea
PROCEEDINGS
of the Marine Safety & Security Council
Winter 2014–2015
Cybersecurity
Vulnerabilities
Threats
Risk Management

COMPARING STUDIES

Vulnerabilities and Potential Consequences

- Vulnerabilities exist, with potentially harmful consequences to ports
  - Industry is migrating toward a more connected control infrastructure and is thus increasingly vulnerable to attacks (TSWG)
  - Security at terminals also involves the use of types of systems for communications, sensors, and command and control (TSWG)
  - Attacks specific to cyber systems can have impact extending into the physical, business, human and environmental systems to which they connect (TSWG)
  - Attackers have targeted global oil, energy, and petrochemical companies, with intent to steal sensitive information such as operational details (OITS)
  - Cyber threats are a growing menace, with potentially "disastrous consequences" for European ports (ENISA)

COMPARING STUDIES

Risk Assessments

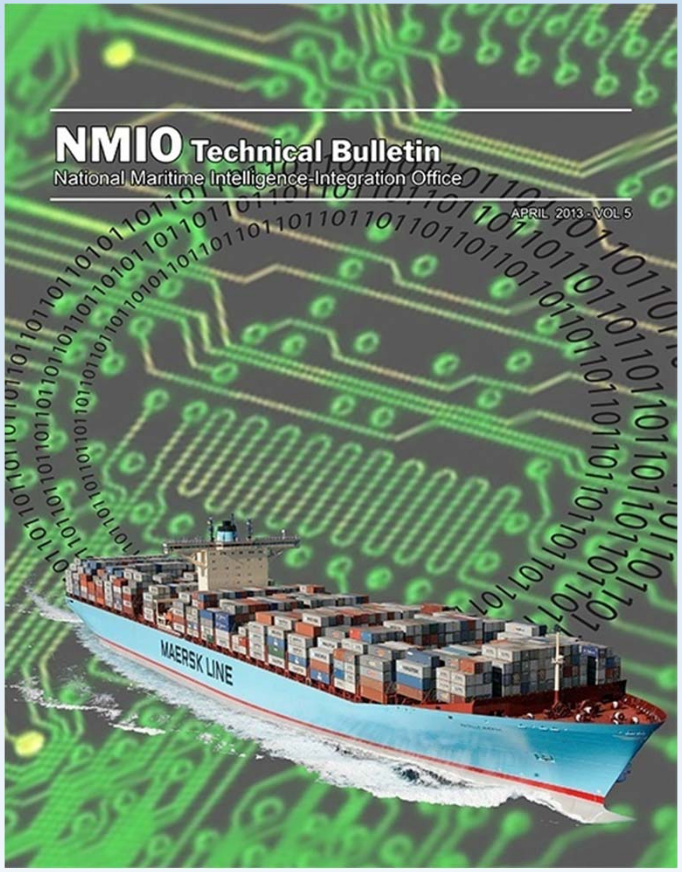
- Risk assessments to date have generally focused on physical (not cyber) security
  - Many Industrial Control Systems used today were designed for availability and reliability during an era when security received a low priority (TSWG)
  - Current maritime governance considers only physical security (ENISA)
  - Of 6 ports, only 1 had conducted a cyber vulnerability assessment, and none had developed a cyber response plan (Brookings)
  - The last National Maritime Strategic Risk Assessment did not address or provide any information on cyber risks (GAO)
  - Without an assessment of cyber-related risks, USCG and its stakeholders will be less able to plan and allocate resources to protect maritime transportation (GAO)

THE VOICE OF THE INDUSTRY
SEAPORTS
AAPA
THE OFFICIAL PUBLICATION OF THE AMERICAN ASSOCIATION OF PORT AUTHORITIES • WINTER 2013 – VOLUME 31
MAGAZINE
aapaseaports.com • aapa-ports.org
SECURING SEAPORT CYBERSPACE
PLUS
CES OPERATORS WORK IN PARTNERSHIP WITH PORT COMMUNITIES
MCCs KEEP PORTS RUNNING IN CASE OF EMERGENCY
ADOLPH OJARD: FORGING HIS OWN PATH

COMPARING STUDIES

Threat Information Sharing

- Threat information sharing is ad hoc and needs to be improved
  - Information exchange platforms should be considered and developed to identify major and upcoming cyber threats (ENISA)
  - At offshore oil and gas companies, both executives and operators must be able to identify the information most critical to business integrity and continuity (OITS)
  - The degree which U.S. information-sharing mechanisms were adequate and shared cybersecurity information was mixed (GAO)
  - The absence of an adequate national-level mechanism to maintain awareness among all maritime stakeholders at various locations reduces opportunities to mitigate cyber-based threats (GAO)

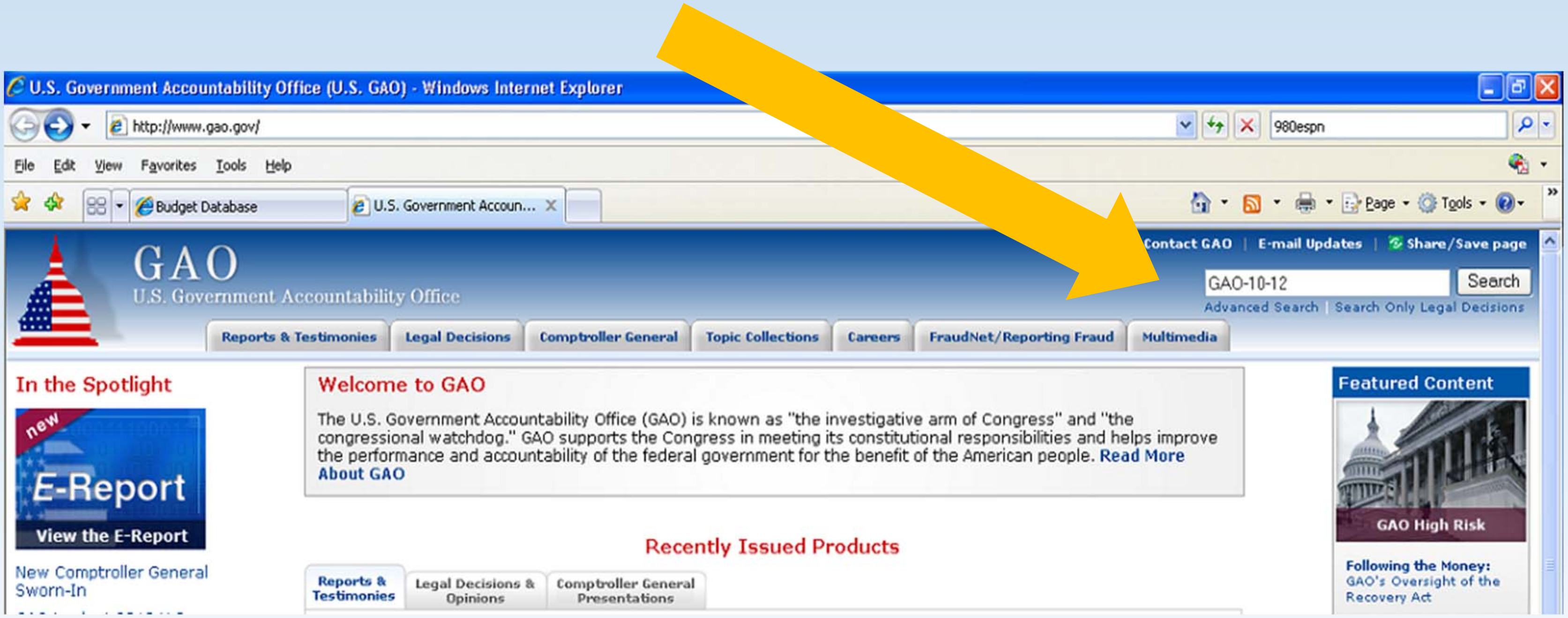


QUESTIONS AND CONTACT INFO

Questions?

Stephen Caldwell, (301) 602-0794, email: stephencaldwell1000@gmail.com

For access to referenced GAO reports, see GAO website: www.gao.gov



Welcome to GAO

The U.S. Government Accountability Office (GAO) is known as "the investigative arm of Congress" and "the congressional watchdog." GAO supports the Congress in meeting its constitutional responsibilities and helps improve the performance and accountability of the federal government for the benefit of the American people. Read More About GAO