Explanation: I compiled the following 37 pages of notes while attending the 4th Annual International Conference on Public Safety: Technology and Counter-Terrorism in San Francisco, CA from 14-15 March, 2005. They are not intended to be complete and I do not claim accuracy. They were prepared for personal use only.

Lieutenant Rachael Bralliar
U.S. Coast Guard
7 April 2005

DAY 1 OF 4TH ANNUAL INTERNATIONAL CONFERENCE ON PUBLIC SAFETY: TECHNOLOGY AND COUNTER-TERRORISM:
14 March 2005

TOM GEDE, EXECUTIVE DIRECTOR, CWAG (CONFERENCE OF WESTERN ATTORNEYS GENERAL)

Conference:

- designed to use interagency methods to exchange information
- increase international understanding and cooperation
- joint operations critical to counter terrorism
- securing borders while maintaining flow of commerce

DAY 1 OF 4TH ANNUAL INTERNATIONAL CONFERENCE ON PUBLIC SAFETY: TECHNOLOGY AND COUNTER-TERRORISM:
14 March 2005

GEORGE TENET, FORMER DIRECTOR CIA:

- "al Qaeda is evolving around the world"
- N. Korea poses a threat to the world
    - Importance of nuclear capabilities
    - because surrounding countries "will mimic if we don't do something about it"
- Muslim/Arab world is "exploding with young men"
    - Demographics and social conditions in these areas directly affect what we're fighting
- 3/4 of central management structure of al Qaeda has been captured
    - discussed what's been done to capture terrorists
    - disrupted 100's of plots
    - made arrests
    - seized documents on how al Qaeda thinks, functions, etc.
- Unless there is international security, the strong security shared by U.S. and Canada does not matter
- History is important because al Qaeda/terrorists "always return to the same methods"--even if they are thwarted
- We are "fighting an enemy that is every bit as good as any international intelligence agency around the world."
- The enemy we are fighting "has an Arab face, and Asian face, and American face, and a Canadian face
- al Qaeda spans it reach around the world
- Indonesian-based al Qaeda pose a possible problem in Asia
- Consider non-Arab English speakers: "Stop looking for Arab faces alone"
- al Qaeda is a "smart and agile organization"
    - "economic and psychological attacks"
    - anthrax, WMD, hydrogen cyanide, etc.
    - "history matters to al Qaeda"
    - "only choice is quiet and patience cooperation . . . to deny al Qaeda funding, people, and political agenda"
    - for "long-term success [we] have to address circumstances in the world that arise and give terrorists opportunities" and that "create opportunities for terrorists to thrive"
        - vast numbers of young men
        - high unemployment
        - "beleaguered states" that cannot control and protect their borders--"in half of these countries, terrorist organizations thrive"
- Intelligence and terrorism in D.C.
    - "capabilities matter"
        - infrastructure linking foreign and domestic intelligence was not in place pre-9/11
    - answer to stopping terrorism

        - NOT more layers of bureaucracy
        - Need speed, agility, "seamless flow of data to American/Canadian private sector" → control what terrorists will target
        - long-term success is not unilateral
            - need "coalition of the willing"
        - "play defense as well as you play offense" → did not exist pre-9/11
            - in playing defense, must constantly increase the "cost of business" for terrorists
            - consider al Qaeda's interest in historical plans
            - systematic, integrated and linked offense and defense is crucial, and the "key is data"
                - need communication built domes to collect, aggregate, etc.
                - more data "where smart people will know how to act when they see something" dangerous
                - need to educate on what we learn, how we learn about it (sources), and open up a wider dialogue
    - al Qaeda counts on anticipation that "we will lost our political will"
- We have to change the paradigm in which there are leaks every time data is discovered

DAY 1 OF 4TH ANNUAL INTERNATIONAL CONFERENCE ON PUBLIC SAFETY: TECHNOLOGY AND COUNTER-TERRORISM:
14 March 2005

ROBERT BONNER, COMMISSIONER CBP:

- discussed 24-hr rule, CSI and C-TPAT
- Dec. 16, 1917 Port of Halifax in Canada is example of port security breaches (accidental collision involving container ship and subsequent explosion)
- Terrorism explosions may necessitate closing all N. American ports because of fear of similar attacks, UNLESS there's a system to defend and protect
- Creation of DHS w/3 missions
    - prevent future terrorist attacks
    - protect truly critical infrastructure
    - respond to terrorist attacks
- CBP = single, unified agency in DHS responsible for our borders
    - clear all entering for all purposes
    - broad customs authority to search, detain and deny admission into the U.S.
    - consists of 40,000 people = 1/4 of DHS
    - developing a comprehensive strategy to secure borders
    - Post-9/11 virtually shut down our borders
        - strategy for security w/o shutting down our economy
- Threat = al Qaeda and associated organizations (jihad Islamists)
    - targeting the world trade
    - trying to acquire nuclear device or components and biological warfare
    - "For the most part" the weapons that they want to use are "difficult to obtain in the U.S. and Canada," and "for the most part" al Qaeda are "outside our borders"
    - CBP's #1 priority is to keep terrorists out of our country
    - We know that terrorists are trying to infiltrate into the U.S. through Mexico and Canada
    - CBP must keep WMD out of our country
    - "shipments may contain terrorist operatives or terrorists themselves"
- Need strategies to detect and prevent WMDs, dirty bombs, nuclear devices, etc
- Containers
    - 25,000 containers arrive in U.S. ports each day → just over 9 million a year
    - containers are "potential Trojan horses of the 21st century"
    - no alternate backup system to container shipments is large enough to take the burden
- CPB twin goals = security and facilitation
- 4-Part Maritime Strategy:
    - 24 hr. rule: advanced information before containers are loaded onto ships in foreign ports
    - Automated Targeting System at National Targeting Center evaluates and identifies potential threats of each container and vessel
    - CSI identifies and targets high risk containers and is operational in 35 of the largest ports worldwide

    - C-TPAT: companies increase the security of their supply chains from loading docks to U.S. for faster processing
        - 8300+ companies participate in program, covering 42% of all imports into the U.S. by value
- Vast improvements in technology at ports of entry to better detect terrorist weapons, particularly WMD
- Oakland is the 3rd largest U.S. seaport and the 2nd largest on the west coast
- Steps to make maritime trade more secure
    - implement smart box
        - secure box with imbedded electronic security device which allows inspectors to determine if it was opened or tampered with
    - Expand CSI
    - take C-TPAT to the next level, more secure information at the point of loading containers
    - Information available to CBP to better identify high risks
    - single window of data shared through ACE
    - Seeking through WCO for all 164 member governments, 4 elements that are internationally recognized in the U.S./Canadian movement of cargo
        - private sectors need one set of standards to comply with
        - improve overall efficiency
- American Shield Initiative
    - personnel and technology to protect land borders
    - improve technology available to CBP and able to detect and understand breaches

DAY 1 OF 4TH ANNUAL INTERNATIONAL CONFERENCE ON PUBLIC SAFETY: TECHNOLOGY AND COUNTER-TERRORISM:
14 March 2005

ROBERT WRIGHT, NATIONAL SECURITY ADVISOR TO THE PRIME MINISTER AND ASSOCIATE SECRETARY TO THE CABINET, PRIVY COUNCIL OFFICE, GOVERNMENT OF CANADA

- Discussed Canada's National Security Policy
- "Smart Borders" process launched between U.S. and Canada
- Comprehensive National Security Policy
    - assesses threats to Canada (terrorist threats are not new to Canada)
    - al Qaeda specifically targeted Canada
    - ongoing engagements with every community in Canada; each community is informed and participating
- 3 core objectives
    - secure Canada and Canadians here and abroad
    - ensure that we're not a threat to our allies
    - provide security abroad
- 4 Parts to Canada's Integrated Approach
    - effective threat assessment and integrated system that is up and running
    - integrated response to threats to protect and prevent
    - integration of consequence management, and coordination of all responses
    - evaluation and oversight

  → all must be connected to U.S. and allies
- 6 Areas identified as gaps in response and what Canada's done about it:
    - intelligence → expanded
    - emergency planning and management
    - public health emergencies → public health agency created
    - transportation security → huge investments, with focus on cargo and maritime security
    - international security → help failed and failing states grow and become part of the world community
    - border security → Manley/Ridge processes have been increased and enhanced; partnerships in technology and engineering
        - Also, Smart Borders Declaration to secure the flow of people and goods, to secure infrastructure, and to coordinate and share information
- North American Security:
    - Canada, U.S., and Mexico engaged in 2003 to broaden and deepen cooperation
        - trilateral objectives with bilateral capability between U.S. and Canada
    - New Partnerships with N. America in Nov. 2004 to advance national and economic security
    - Maritime NORAD: common domain awareness, protocols for dealing w/threats, etc.

DAY 1 OF 4TH ANNUAL INTERNATIONAL CONFERENCE ON PUBLIC SAFETY: TECHNOLOGY AND COUNTER-TERRORISM:
14 March 2005

(BUSINESS BRIEFING)
TODD WISEMAN, VICE PRESIDENT, HOMELAND SECURITY, IBM FEDERAL:

- **3 Objectives of Technology Solutions for Border Security:**
  - facilitate legitimate travel and trade
  - manage protection of nation's borders
  - assure secure supply chain
- Share, collaborate, and leverage information across sources
- Typical application architecture focuses exclusively on DHS, State, and local governments/communities
- Importance of open standards
  - fuse business and information technology
  - business model component for DHS

DAY 1 OF 4TH ANNUAL INTERNATIONAL CONFERENCE ON PUBLIC SAFETY: TECHNOLOGY AND COUNTER-TERRORISM:
14 March 2005

ROBERT SCHOCH, DEPUTY ASSISTANT DIRECTOR OF NATIONAL SECURITY INVESTIGATIONS, U.S. IMMIGRATION CUSTOMS ENFORCEMENT (ICE)

- discussed 1994 Chinese smuggled via container ship in SF Bay
- emphasized focus on domestic and international crimes
- discussed revamping methods to track U.S. visa violators, foreign students, etc., as well as theft of military equipment by terrorists
- ICE Investigates under the Patriot Act to dismantle funding of terrorists (how they earn, move, and store $)
    - al Qaeda spent <$500K collectively in planning and executing the 9/11 attacks
    - capture alien smugglers by seizing their $ and assets used for human trafficking
    - 56 foreign offices worldwide
        - investigate crimes crossing borders
    - terrorists "continue to plot" and use "more technologically sophisticated" means
        - ICE provides additional defense
    - comprehensive foreign student tracking (9/11 hijackers all had "student visas")
        - student and exchange visa violators → CEVIS program to follow those who violate student visas
        - notification systems are immediately entered
    - border and transportation security → BTS
        - monitors entry and exit of foreigners into U.S.
        - biometrics collected by CBP at borders
- Along with DoD and DHS, ICE enters biometrics of enemy combatants encountered overseas
    - biometrics is checked against watch lists
    - "Unknown Threat" → ICE has a threat analysis infusion center
        - threat analysis reviews all who are refused access to U.S.; ICE looks for domestic links to people in the U.S.
- Office of Visa Security: reviews suspicious visa applications for fraud and to see who poses a high risk

DAY 1 OF 4TH ANNUAL INTERNATIONAL CONFERENCE ON PUBLIC SAFETY: TECHNOLOGY AND COUNTER-TERRORISM:
14 March 2005

INTERNATION SHARING OF LAW ENFORCEMENT INFORMATION: PANEL DISCUSSION:

- **John Neily, Assistant Commissioner, Criminal Intelligence Directorate, Royal Canadian Mounted Police (RCMP) :**
  - discussed challenges in information sharing
    - protecting the privacy of those about whom we have collected information
      - how to protect those whose information we have collected and
      - how to insure protection of information that we share with others
  - "if another nation refuses security clearance . . . we must have that information
  - DNA is a very sensitive issue
    - must deal with accountability and reliability of agencies and countries if we decide to share DNA information
- **Phillip Webb, CEO, Police Information Technology Organization (PITO), U.K.:**
  - "key point is delivering the right information to the right person in the rights amount of time"
  - discussed biometrics to detect and identify
  - U.K has fingerprinting and palm database
  - National biometric system for all U.K. forces will be implemented 1 April 2005
    - roadside fingerprinting
    - working on mugshot ID and videotaping
  - National Identification Card in 2008
    - facial image and fingerprints and iris scan
    - to be required of all U.K. citizens
  - Passports and drivers licenses have biometrics
  - "need to have a wider debate on what should be done rather than what can be done"→ "is it right to exchange personal information?"
  - Police services coordinate across the board
  - NAFIS Biometric Management System: has 6.2 Million records
    - biometrics taken at time of arrest and information is kept indefinitely
    - also have a national violent sex offender biometric system
  - PLX: Police local cross reference biometric data
  - SIS: Schengen Information System
  - Central Information Service: pools databases locally, regionally, and (by the end of this year) nationally (through National Data Exchange System), and regarding infrastructure (must be accurate and secure)
    - must consider existing ethical considerations
    - consider reciprocity and whether the information was intended to be used and disseminated → "who 'owns' the information?"
    - problems are not technical now, but are legal and ethical
  - "passports can be obtained or forged easily"
    - "we need a biometrics that can actually prove you are who you are."
    - DNA is collected from anyone arrested in the U.K.

- **John E. Lewis, Deputy Assistant Director, Counterterrorism Division, FBI**
  - discussed changes within the FBI to further information exchange with countries around the world
  - sharing of information "will be the hallmark of our success to counter terrorist"; such information was previously only used for crimes
  - Investigation Data Warehouse (IDW): gives information on known and suspected terrorists
  - Integrate Automated (???): system of fingerprints collected around the world
    - law enforcement, military and DHS can be access this database
  - "Training is vital: information doesn't help if we don't know how to use it"
    - we share information with other countries and train other countries on how to use it
  - LEGATS: legal association through the world, located overseas
  - FBI: Working on financing angle of terrorism, how to end terrorist organizations by cutting of funding
  - Working w/Russia to share information and discuss strategies
  - International work to counter domestic extremist groups, such as eco-terrorists (e.g. ALF (animal rights), ELF and SHAK (?) (huntington life sciences)
  - Cooperation among international partnerships has broken up many terrorist cells
- **Edgar MacLeod, Canadian Association of Chiefs of Police (CACP):**
  - "information can be shared for a variety of purposes, by a variety of people, including criminals"
  - Nov. 2003 Information Committee Conference -- discussed how to overcome barriers to information sharing
  - Information = "data and the collection of facts with meaning connected to those facts"
    - trained analysts understand the information
    - "information is the lifeblood of police work"
    - "information is analyzed and it's intelligence"
      - purpose of analyzing the information is to protect citizens "within the country and beyond"
      - there is no clear dividing line between police and other law enforcement activities
  - Canada limits how police and law enforcement agents collect, hold and disseminate information
    - however, National information is different because the rights of the individual depend upon who has the information
    - "When everyone's responsible, there's a question of who's accountable."

DAY 1 OF 4TH ANNUAL INTERNATIONAL CONFERENCE ON PUBLIC SAFETY: TECHNOLOGY AND COUNTER-TERRORISM:
14 March 2005

(Business Briefing) MARK BORNAIS, DIRECTOR OF PUBLIC SAFETY AND EMERGENCY PREPAREDNESS CANADA:

- Canada created an information-sharing system with interoperability
  - not just technological
  - involves culture, law and is extremely complex
  - interaction at many levels and through many layers
  - contains nexus and fast programs to protect without impeding business
- Interoperability Maturity Model: assesses agency's abilities to achieve interoperability
- Building a national strategy for radio interoperability
  - gives first responders the capability to provide and receive information
- Sharing primary records
  - LEAQ: Law Enforcement Quarterly
  - lets law enforcement responders know what's waiting for them when they respond (e.g. if classified information shows that nuclear or radiological components are on site, we want them to have that information to respond safely and appropriately)

DAY 1 OF 4TH ANNUAL INTERNATIONAL CONFERENCE ON PUBLIC SAFETY: TECHNOLOGY AND COUNTER-TERRORISM:
14 March 2005

(Business Briefing) NED AHEARN, PARTNER, NORTH AMERICAN SUPPLY CHAIN MANAGEMENT, UNISYS CORPORATION:

- Global and secure commerce and business solutions
    - involved in Operation Safe Commerce (coordinated by Unisys), TSA efforts, Passport programs, TWIC, etc.
    - worldwide trade ➔ Huge business
        - global gross product in 2003 = $36 Trillion
        - anticipated that global gross product in 2025 = $50 Trillion
    - Security adds to complexity. But, consider:
        - future green lanes for C-TPAT and CSI companies/ports
            - implementation anticipated by the end of the year
        - WTO adoption of DHS approach
- Remaining question of what to do with all the information we're getting (much of which is wireless)
- Key Success Areas
    - prevent terrorist attempts
    - detect threats
    - respond
    - have an infrastructure that enables us to do all those things
- Takeaways:
    - establish your priorities
        - physical controls
        - relationship controls
        - information controls
    - engage labor
    - address considerations
    - integrate solutions
        - congestion flow vs. ability to execute
        - access control
        - emergency data
    - leverage emerging technologies
        - "When bad things happen, communications aren't there anymore"
    - leverage best practices while focusing on the blind spot
    - adopt and adapt: get infrastructure and technology right

DAY 1 OF 4TH ANNUAL INTERNATIONAL CONFERENCE ON PUBLIC SAFETY: TECHNOLOGY AND COUNTER-TERRORISM:
14 March 2005

JACQUES DUSHESNEAU, PRESIDENT AND CEO, CANADIAN AIR TRANSPORTATION SECURITY AUTHORITY (CATSA)

- New advancements to meet new challenges in airport security
- "New terrorism is arising all over the world"
    - discusses our dependence on technology and the pitfalls of such reliance
    - terrorism post-9/11 is much more amorphous and diffuse
    - new terrorist groups:
        - shadowy international network
            - mobilize part-timers, with no police record or involvement, etc
            - problems with detection
        - no negotiation interest
            - do not want to change the system
            - seek to destroy the system
        - extremist ideologies
- Ingenious Terrorists: when security measures are put into place, terrorists are "there the next day" finding a way to "go around" it.
    - focus on finding our weaknesses and using our strengths against us
    - the spread of technology allows for greater organization of terrorist cells
- Targets
    - real target of terrorists is the human mind/psyche; inflict disorder upon the collective psyche
    - media becomes an accomplice as a vector of fear
- Infosphere
    - with the advance of information technology, particularly cyberspace, there have developed changes in how information is dispersed and planned
    - there's a close connection between infosphere and cyberspace (e.g. videos of executions by terrorists posted on the web)
- Dependence upon technology
    - technology makes our work easier
    - however, technology is limited, as seen in the security failure in the 9/11 attacks
        - e.g. local NYC authorities ordered evacuation after the 1st tower collapsed→21 mins. later, the North tower collapsed and many killed because of failure in communication
    - growing dependence on technology, especially computers is not foolproof
        - no computer system is safe
        - hacker tools are increasingly easily accessible
        - spyware indicates "a new breed of enemies"
        - enemy has the same tools that we do
        - the same IT learning tools that are developed are used against us (e.g. 9/11 and Madrid attacks. Madrid terrorists used internet chat groups to plan over the course of only three weeks)

        - "computer is a stealth weapon"
    - al Qaeda has information technology and is willing and able to exploit it
        - demonstrated innovative development of new weapons
        - "information technology attack is a matter of 'when,' not 'if'"
- must improve quality, not just increase security
    - "effective security is a work in progress"
    - "we do not have the luxury of error"
- Pooling systems of information management prevents duplication
- "take a lesson from the terrorists" in reorganizing how we operate → decentralize
- "we must be more than proactive, we must be preemptive"
- Message: while technology can do a great deal for securing our community and country, it can also pose problems. We must through of the weaknesses in technology and how to address them

DAY 1 OF 4TH ANNUAL INTERNATIONAL CONFERENCE ON PUBLIC SAFETY: TECHNOLOGY AND COUNTER-TERRORISM:
14 March 2005

CAROL DiBATTISTE, DEPUTY ADMINISTRATOR, TRANSPORATION SECURITY ADMINISTRATION (TSA), DHS:

- TSA Mission = to secure the entire transportation system without impeding flow
  - define critical assets
  - determine how vulnerable the assets are
  - mitigate risks
- Discussed the use of technology to enhance aviation security and mitigate risks by focusing on:
  - leadership of people, technology, and constantly transforming to meet the threats faced
  - partnerships
  - friendships: customer service is vital to achieve a proper balance between security and personal freedoms (protecting privacy)
- Registered Travelers: allows expedited screening in aviation of pre-registered travelers
  - enhanced security measures
  - tests biometric technology (e.g. iris and fingerprint scans)
  - expedites screening process for passengers
  - privacy safeguards are in place to protect data
- TWIC: controls access to ports or airports (in the works)
  - Aviation: "we're in the 3rd phase, the prototype phase" for aviation ID cards
    - already completed aviation technology phase
    - currently testing TWIC at select airports
    - in the prototype phase, the employer specifies where a person has access after biometric identification verifies who the person is
    - currently looking into limitations of issuing TWIC cards (what crimes prevent)
    - anticipating May 2005 completion of TWIC prototype
      - TSA is "constantly meeting with our partners to coordinate and control access"
    - Air Cargo security → inspections have tripled
  - working with U.S. Coast Guard "to get rule-making for TWIC maritime workers"
    - "trying to get it done within the next year"
- Other Programs (again, these are all in the works)
  - Known Shipper databases
  - Cargo Strikes → unannounced inspections to confirm compliance with security measures in place
  - Freight Assessment program: targeting high-risk cargo through automated systems and implemented through the use of technology
    - implementation anticipated in 2006 or 2007
    - currently in the midst of developing a prototype
  - Airport Access Control Pilot Programs
    - testing is in the 1st Phase

        - involves state-of-the-art technological security around airport perimeters and controlled access in and outside of airports
    - EVS and Baggage Screening technology
    - Explosive detection devices
        - currently being tested in labs
        - looking for technology to replace "pat down" inspections
        - e.g. puff of air can establish if you've been exposed to explosives
        - Document scanner of boarding pass shows if anyone who touched the boarding pass was exposed to explosives
    - Working on innovative financing and cost-sharing alternatives
    - Secure Flight is the next generation of aviation security
        - being tested now
        - puts watch lists in the hands of the federal government and automates screening of passengers
        - reduces in half the number of people selected for pre-screening
    - International programs are vital to security partnerships
        - must consider who will be the 1st on site to respond to an attack
        - TSARs are TSA points-of-contact located overseas in 14 different countries to help assess activities

DAY 2 OF 4TH ANNUAL INTERNATIONAL CONFERENCE ON PUBLIC SAFETY: TECHNOLOGY AND COUNTER-TERRORISM:
15 March 2005

ADRIAN BACIU, INTERPOL BIO-TERRORISM UNIT (OIPC), LYON, FRANCE:
World expert on bioterrorism.

- Bioterrorism differs from chemical, radiological, and nuclear terrorism because it:
  - can be replicated and has multiple capabilities
  - is difficult to detect on-site
  - can be carried by a human being, animal/insect, or from food growth cultures
  - is difficult to distinguish between naturally incurring outbreak or criminal act
- Biological threat scenarios include war, terrorism, or criminal acts
  - Small quantities are enough, easy to hide and smuggle.
  - Can be freeze-dried and smuggled
  - Chemical weapons components are controlled and leave "telltale signatures"--biological agents are available for other legitimate purposes
  - No hand-held detection device: those first responders are exposed
- Port vulnerabilities to biological agents:
  - small quantities effective in large, opened area ports
  - easy access to ports by land or water
  - metropolitan area neighborhood--lots of people
  - transportation links to other locations
- Port Challenges:
  - Safeguard Systems Implementation
  - Financial Resources Needed
  - Cooperation and Coordination
- Potential Answers:
  - risk assessment
  - enhanced surveillance
  - realistic deployment of assets, etc.
- Risk Sources
  - information available on internet for terrorist targeting
  - sensitive information sharing
  - operation confidentiality
  - vulnerability assessment
  - containment plans
  - health community involvement
  - responsibility area limitation
- Risk Profiles: countries of concern--which ones comply w/law?
- Interpol's three-core functions
  - secure global police communication services
  - operational data services and databases for police
  - operations support services
- Global Police Communications Systems: internet protocol w/highest levels of security and priority
  - full messaging system (w/biometrics)

    - web tools for police purposes
    - access to databases
- Law Enforcement Program Areas--cover a broad range of crimes
    - Databases w/those who may be involved in such activities
- Discussed threat of easy food contamination/animal contamination
- Interpol Conference on Bioterrorism held 1-2 March 05--working on operational support of member states
- Need International Cooperation: currently, many organizations are trying to do same thing, either regionally or internationally
- Need information and data sharing: fingerprints, DNA, biometrics, etc.

DAY 2 OF 4TH ANNUAL INTERNATIONAL CONFERENCE ON PUBLIC SAFETY: TECHNOLOGY AND COUNTER-TERRORISM:
15 March 2005

NOEL K. CUNNINGHAM, DIRECTOR, OPERATIONS AND EMERGENCY MANAGEMENT, PORT OF LOS ANGELES:

- Two of the largest U.S. ports are in CA, and L.A. is world's 3rd largest port complex (Singapore is largest, Long Beach is 2nd)
- Worldwide Port Statistics:
  - $200 Billion annual trade
  - >2 Million jobs
  - 12 Million containers annually
  - 43% containers entering US Ports
- Port facilities and terminals: passenger, oil and chemical, container, and other freight.
- Transportation Infrastructure: inter-modal trans hub, bridges, ships channels and waterways, and marine facilities and terminals
- Port Security Operations: foundation is w/harbor, shore and air patrols. Vessel escorts, including cruise ship industry, vessel boardings, dive operations--underwater dive operations (randomly done on cruise ships), multi agency cooperation
- "An attack on the cruise ship industry would probably kill that industry"
- MARSEC (Maritime Security) Levels
- Area Maritime Security Committee: established in March 2004 under MTSA
  - includes law enforcement, emergency response, port stakeholders
  - coordinates operations, intelligence sharing, training, and planning
  - developed Area Maritime Security Plan
- Security Infrastructure
- Credentialing "is probably the weakest portion of our security" --there currently is no bona fide seaport type credential
  - TWIC is developing prototype for maritime identification program
- Waterside Surveillance: underway
- World Cruise Center: perimeter security enhancements; vehicle screening
- Port of Administration (POLA) Facilities: must secure our headquarters
- Promenade for tourist attractions: Security needed
- Supply Chain Security
  - CBP Initiatives
  - CSI
  - C-TPAT
  - Radiation Portal Monitors
  - Operation Safe Commerce
  - Joint ???
- LA/LB Approach: biggest concern is to not simply purchase technology. We need a technological approach that will work, secure our nation, and keep commerce moving
  - Sandia is used to develop security technology
  - Joint Container Inspection Facility: (result of efforts from Sandia and CAPT Neffenger) when a container arrives in port, it is placed on freeway and travels.

        - under Joint Container Inspection Facility, first responders will be on the waterfront at a multi-agency container inspection station. Will integrate into port operations.
- Operation Safe Commerce:
    - focuses on point of origin in supply chain,
    - is considered as guidelines but respects state sovereignty: 4 supply chains, 514 Containers
- PSA, Unisys, Boeing
- Technology:
    - Radio frequency ID Tags: RFIDs
    - GPS tracking
    - real-time notification systems
    - high security container locks
    - e-seals
    - CBRNE detection

DAY 2 OF 4TH ANNUAL INTERNATIONAL CONFERENCE ON PUBLIC SAFETY: TECHNOLOGY AND COUNTER-TERRORISM:
15 March 2005

REAR ADMIRAL (NS, SINGAPORE) LUI TUCK YEW, CHIEF EXECUTIVE MARITIME AND PORT AUTHORITY OF SINGAPORE:

- 4-pt framework:
  - ISPS Code
  - Securing port waters--additional sec. measures beyond ISPS. IMO, e.g.
  - Securing SLOCs
  - Supply Chain Security--global supply chain
- ISPS Code:
  - 1/4 commerce and
  - 1/2 world oil through Singapore ports
  - Singapore was one of the first ports to comply
- Transnational Security measures--"only as strong as the weakest link"
- More efforts to maintain and improve security
  - test readiness
  - identify and close loopholes
  - share and disseminate best practices
  - "no room for complacency" "a bad day . . . can be the last day"
- Random audits are done
- ISPS deals only w/ships >500 gross tons
- Beyond ISPS Code, Securing Port Waters:
  - security guidelines for small vessels w/self-inspections and follow-up by inspectors
  - IMO mandates AIS for all vessels
  - HARTS: Harbour Craft Transponder System (going to be mandated on all Singapore ships--monitor, ID and check 98% vessels in port, allows focus on vessels w/o electronic ID)
- Other measures:
  - designated routes
  - movement away from "sensitive vessels"
  - Securing SLOCs: "if sea lines of communications are arteries of global commerce, then Malacca and Singapore Straits are the jugular vein"
    - discussions on regional maritime security are gaining momentum
    - developing consensus
      - primary responsibility lies w/littoral states;
      - but all stakeholders play a role, to consult and conform with international law
  - UNCLOS: need to look at it again
    - piracy has increased since UNCLOS codified in 70's
    - terrorism not addressed
    - "not as current as we need it to be"--needs to be updated to deal w/threats today
  - Cargo/Supply Chain Security:

        - ports and ships only one link in "global supply chain"
        - consider how cargo is handled before it is loaded on a ship
- Measured approaches:
    - 1 view = total achievable at all costs
    - OUR VIEW = it is "more realistic to strike balance between needs of commerce and security and a targeted risk management approach"
- Risk Management
    - risk-profiling key element
    - information on nature, origin, transportation, destination, etc. of cargo is needed
    - better chance of identifying patterns, anomalies deviations--is route normal or deviated?
- Content Security:
    - Secure what is inside box, not just box itself
    - need to create sufficient incentives for every player along supply chain
    - lessons from air cargo sector: "known shipper regimes" should be standardized and applied to ports
        - People in supply chain: vigilance is a better view than focusing on crew members as "potential terrorists"--may lead to widespread ill will. We need them to work w/us.
- Seafarer ID by ILO:
    - necessary but insufficient
    - doesn't address background of seafarers
    - crewing agencies, etc., are crucial and we need accreditation measures from those who hire seafarers

DAY 2 OF 4TH ANNUAL INTERNATIONAL CONFERENCE ON PUBLIC SAFETY: TECHNOLOGY AND COUNTER-TERRORISM:
15 March 2005

REAR ADMIRAL KEVIN ELDRIDGE, COMMANDER U.S. COAST GUARD, D11:

- Changing nature of missions since 9/11
- Overview: moved from response to presence organization
    - Multi-mission maritime services
    - oldest sea service (fought every major U.S. Conflict)
    - pre-9/11 response
    - post-9/11 presence
    - Closing D11 would cost >$1 billion per day
- 2 priority missions:
    - Maritime Homeland Security
    - Search and Rescue
- Terrorist goals: fear and harm economy
- USCG Port security efforts:
    - 2% pre 9/11
    - 50% right after 9/11
    - 25% today
- Today's challenges: mission balance
- USCG efforts to reduce terrorist risk:
    - inc maritime domain awareness
    - implement
- HLS Strategy:
    - increase maritime domain awareness
    - implement layered defense, etc.
- Since 9/11:
    - increase in advance notice for vessels >300 gross tons from 24 to 96 hours→in addition, more information is required
    - increase in air and harbor patrols to increase maritime domain awareness
    - expanded intelligence coordination
    - enhanced VTS, using AIS technology
        - automatic identification systems
        - provide an operating picture for vessels operating near U.S. shores and inland maritime domains
    - deepwater project to retrofit our assets
    - building first National Security Code set for release in 2007
    - USCG Commandant created a group at headquarters to address threats and to team with the Navy to increase maritime domain awareness
- USCG use of technology to develop a layered defense
    - in foreign ports:
        - CBP--agents in 34 of the largest ports
        - CSI (cargo manifest are required 24-hrs before containers are loaded on ships)

    - during transit:
        - surveillance technology allows interdiction on the high seas if problem arises
            - cannot yet track and intercept to level desired
        - Sea Marshals:
            - maintain positive control to prevent takeover as vessels approach our ports
            - look at the country of origin, crew, cargo, and intelligence
            - boarding determinations are made by the local COTP
        - MSSTs: 100 person units
            - highly trained for anti-terrorism and force protection
            - 13 teams nationwide
            - capabilities include:
                - dive teams
                - K-9, bomb dog teams
                - anti-swimmer systems
                - radiation detection equipment
    - deterrence: USCG is more of a "presence organization" than pre-9/11
    - Area Maritime Security Committees, as required under MTSA
        - chaired by USCG COTP
        - members include industry, etc.
        - ensure readiness to respond
- USCG HLS Strategies:
    - increase maritime domain awareness
    - implement layered defense
    - increase operational presence and inter-agency partnerships
    - ensure readiness to respond

DAY 2 OF 4TH ANNUAL INTERNATIONAL CONFERENCE ON PUBLIC SAFETY: TECHNOLOGY AND COUNTER-TERRORISM:
15 March 2005

MARC GREGOIRE, ASSISTANT DEPUTY MINISTER, SAFETY AND SECURITY, TRANSPORT CANADA

- Canada's Marine System
  - over 200K km of coastline
  - 3 main ports
    - Vancouver
    - Montreal
    - Halifax
- Maritime Security Responsibility--key Canadian Federal departments are responsible for maritime security
  - Transport Canada
  - National Defense
  - Public Safety and Emergency Preparedness Canada
    - Canadian Border Service Agency
    - Canadian Security Intelligence Service
    - Royal Canadian Mounted Police (RCMP)
  - Canadian Coast Guard
    - not armed in Canada
    - armed component comes from RCMP
  - implemented 96-hr rule
- Maritime Security Risk Matrix:
  - Foreign Security Zone:
    - domain awareness
    - safeguarding
    - collaboration
  - International Waters Security Zone:
    - domain awareness
    - collaboration
  - Canadian Waters Security Zone
    - domain awareness
    - responsiveness
    - collaboration
  - Coastal/Land-side Security Zone
    - domain awareness
    - responsiveness
    - safeguarding
    - collaboration
- Funding commitments have continued and there is increased presence on the water
- 6-Point plan is in the process of being implemented
- Coordination with the U.S.: Canadian marine security regulations parallel U.S. rules
  - don't want a ship denied entry in one of the countries (Canada or U.S.) to enter via the other

    - bilateral security arrangements: if both countries comply with ISPS Code, the other country does not need to screen it for compliance--compliance is presumed
    - joint initial verification project
    - connectivity of marine security operation centers
- Discussions in progress to work with U.S. on Great Lakes for security
- Canada met the compliance deadline for ISPS Code
    - certificates were issued to 218 vessels
    - certificates issued to 420 marine facilities
- Marine facilities restricted area access under clearance program
    - required security clearance for certain workers
    - regulations by Sept. 2005
    - in process of looking at initial implementation at Vancouver, Halifax, and Montreal
    - balance needed to avoid alienating longshoremen
- Future Challenges:
    - improve integration and communication
    - build trust in application of the ISPS Code
    - enhance waterside and domestic ferry security
    - develop security management system, etc.

DAY 2 OF 4TH ANNUAL INTERNATIONAL CONFERENCE ON PUBLIC SAFETY: TECHNOLOGY AND COUNTER-TERRORISM:
15 March 2005

(Business Briefing) SCOTT J. GLOVER, DIRECTOR, MARITIME SECURITY, HPA, LLC

- discussed tracking compliance
- discussed Container Terminal Expansion
- International Initiatives:
    - SOLAS-ISPS Code (IMO)
    - MTSA
    - ILO: mariner credentialing using a central database of the issuing country to confirm identity
    - WCO framework
        - C-TPAT
        - Operation Safe Commerce
        - CSI
- All but 7 countries have certified compliance with ISPS Code
    - USCG publishes compliance lists
    - but a "cursory examination of some port makes you wonder" if they really comply with ISPS Code
        - it is "not true" that all but 7 countries really were in compliance with ISPS Code by July 1, 2004 deadline
        - however, progress is being made
    - compliance is tracked for U.S. and, effectively, for foreign vessels
- Tracking Compliance so cargo vessels entering U.S. are secure
    - U.S. vessel and facility compliance
    - USCG verification inspections are done initially, and then every 5 years. There are annual follow-up inspection
    - USCG Annual Safety and Security Inspections
    - U.S. does internal audits
- Foreign Vessel Compliance
    - flag state verification: just like with the U.S., done initially and then every 5 yrs thereafter
    - Traditional Port State Controls: boardings are risk-based
- Foreign Port Facility Compliance
    - MTSA 2002 requirements: the USCG evaluates plans to analyze anti-terrorism measures in foreign ports
    - traditional port state control approach is not valid
    - International port security program
    - USCG does assessments in foreign ports even though CBP are already there under CSI
        - working on developing discussions between CBP and USCG at foreign ports

        - "the CBP and USCG are not bumping into each other" but efforts are being made to coordinate with USCG and to use CBP assessments done in accordance with CSI in completing USCG compliance assessments
- Maritime Security Projects of HPA
- Facility Security Plan Reviews
    - USCG implemented centralized review system for all plans submitted
    - reviews 3200 port facility security plans and 9300 vessel security plans
    - result = all plans were reviewed by July 1, 2004 ISPS Code deadline
- TSA Port Security Training Exercises Program
    - conducts exercises at 40 ports
    - major goals:
        - increase awareness of government agencies of critical processes during and after seaport security incidents, etc.
        - integrate information-sharing and response
- Waterside Security
    - standard anti-terrorism vessel collision structures
    - continuous floating security barrier systems to defend against USS COLE-like attacks → HPA is working with the Navy to deploy these barriers that are designed by private companies

DAY 2 OF 4TH ANNUAL INTERNATIONAL CONFERENCE ON PUBLIC SAFETY: TECHNOLOGY AND COUNTER-TERRORISM:
15 March 2005

JEFF BREINHOLT, DEPUTY CHIEF, COUNTERRORISM SECTION, U.S. DEPT. OF JUSTICE:

- Redressing Terrorist Financing through Criminal Prosecutions
  - #1 mission of law enforcement post-9/11 is prevention
  - law enforcement was inserted into terrorist plan
- Problems with terrorist financers
  - they don't look like terrorists; they often are otherwise legitimate professionals who "fund" terrorists
- Criminalizing Terrorism: Problem = There's no federal crime for terrorism
  - Use of social scientists to determine what terrorists methodically do to create crimes that make acts prosecutable
  - public safety crimes
  - crimes that infringe upon constitutional rights
  - must consider:
    - how do financers operate and
    - make that illegal
    - how are charities improperly used to fund terrorists
- Current Solution: There's a published list of terrorist organizations
  - funding these organizations is illegal, cannot claim ignorance or intent to fund only the "good" functions of the organization
  - criminal acts include providing anything of value to these organizations
  - these crimes are upheld against claimed constitutional violations as forwarding legitimate government interests
  - John Walker Lind was charged with providing resources to terrorists, i.e. himself, his body

DAY 2 OF 4TH ANNUAL INTERNATIONAL CONFERENCE ON PUBLIC SAFETY: TECHNOLOGY AND COUNTER-TERRORISM:
15 March 2005

Recent Advancements in the Use of Biometrics for Identification:
RAJ NANAVATI, PARTNER, INTERNATIONAL BIOMETRICS GROUP (IBG):

- Biometrics Group provides biometrics systems around the world
  - projects
  - challenges
  - resolution
- Projects:
  - multiple enrollment detection systems
  - watch-list searches
  - confirmation of identity at port of entry
  - the system processes biometric data very quickly, in a couple of minutes
- CANPASS Air
  - uses biometrics for airport security to remove "low risk" passengers from the screening pool
- NEXUS Air
- TSA Registered Travel Program: based on Aviation Transportation Security Act (ATSA)
- Challenges:
  - Technical (template and image interoperability)
    - common baseline understanding of accuracy
    - common standards
  - Policy Issues: sharing information
    - what type of data should be shared
    - what guidelines should be followed in sharing information
    - need to develop cooperative plans
    - need to resolve different privacy policies
- "This is a technology that has been thrust ahead of its growth curve"
  - we are "just beginning to discover what technology can do"
- Technical Challenges involve compilation of data→is the date compatible
  - fusion combines different biometrics, e.g. fingerprints with facial characteristics
  - needs an independent testing of Iris Recognition Technology (ITIRT)
    - need to test the reliability of this biometric and the failure rate
    - this is done by IBG and will be published soon
- Discussed science and math behind the rate of success in testing to show reliability of system
- Standardization involves an important 4-Part Process:
  - Develop
  - Specify
  - Implement and
  - Conform
- Policy Challenges include:
  - sharing information inter-agency and internationally
  - requires cooperation and privacy framework

DAY 2 OF 4TH ANNUAL INTERNATIONAL CONFERENCE ON PUBLIC SAFETY: TECHNOLOGY AND COUNTER-TERRORISM:
15 March 2005

KEVIN HURST, SENIOR POLICY ANALYST, OFFICE OF SCIENCE AND TECHNOLOGY POLICY, EXECUTIVE OFFICE OF THE PRESIDENT:
khurst@ostp.eop.com

- Biometrics Interagency Working Group (BIWG)
    - Priority objective is to have a National Security Strategy for homeland security
        - biometrics can help accomplish this objective
    - Government is working on biometrics for employees
        - each agency may develop and implement the system it wants, but each system must meet certain consistent guidelines
    - Facial Recognition:
        - currently, don't have the capability for this
        - State Dept is developing a system to use this, but it still requires human intervention and has limited accuracy
        - working on a 3-dimensional model
    - Iris Scans (not retina)
    - Fusion of multiple biometrics: "like any system, if you don't do it right you run the risk of making it worse"
        - trying to reduce error rates and variables that render once source unreliable
        - may provide a barrier to "spoofing"

DAY 2 OF 4TH ANNUAL INTERNATIONAL CONFERENCE ON PUBLIC SAFETY: TECHNOLOGY AND COUNTER-TERRORISM:
15 March 2005

J. CLARK KELSO, STATE CHIEF INFORMATION OFFICE, CALIFORNIA

- "We have a long, long way to go . . . California is not unique in this"
- Cyber-Security is an oxymoron because it is the antithesis of secure
    - problem is that there is no security
    - even those trying to design security measures have been subjected to exposure of personal information
    - there's a problem with identification
    - there's also a problem with management
    - "who has what authority to do what with digital technology" is problematic
    - at the State level, enormous challenges exist to feel an acceptable level of security

DAY 2 OF 4TH ANNUAL INTERNATIONAL CONFERENCE ON PUBLIC SAFETY: TECHNOLOGY AND COUNTER-TERRORISM:
15 March 2005

TODD HINNEN, TRIAL ATTORNEY, COMPUTER CRIMES AND INTELLECTUAL PROPERTY SECTION, UNITED STATES DEPARTMENT OF JUSTICE

- Discussed
  - Global Islamist Terrorism and
  - the Internet
- Questioned the "why, how and what" we can do about terrorists using the internet
- Why terrorists use the internet:
  - anonymous and protected
    - internet offers "security" measures e.g. encryption, etc, as a way to hide a message file
  - inexpensive and easy to use
  - geographically unbounded; "does not respect international boundaries"
  - internet is decentralized; there's no choke point through which it flows, so interception is difficult or impossible
- How terrorists use the internet
  - universal call to jihad
  - al Qaeda websites are hosted on U.S. servers
  - hostage broadcasts/executions
  - as a means of spreading terror
  - pictures of martyrs page, etc, for recruiting
    - wealth and honor for family of martyrs
    - reward for suicidal bombers
  - allows access to ideological community while removing the viewer from the reality of the situation
  - fund-raising and movement of funds: usually done through online "charities"
    - Muslims supposed to donate % to charity each year
    - use of credit card fraud
    - PayPal abuse
    - operational use
  - communicate religious justifications for killings and terrorist acts
  - present information for "terrorist franchises" to use, e.g. how to create suicide bombs
    - shows impact on a simulated passenger bus
    - how to use a rocket-propelled gun
    - manual on botulism toxin
      - paralyzes, then kills
      - very virulent
      - single gram can kill >1 million people
      - guidance online on how to use botulism as bioterrorism
  - online worms and viruses
  - "internet is the perfect medium for a perfect crime"

DAY 2 OF 4TH ANNUAL INTERNATIONAL CONFERENCE ON PUBLIC SAFETY: TECHNOLOGY AND COUNTER-TERRORISM:
15 March 2005

DAVID DOUGLAS, VICE PRESIDENT RISK MANAGEMENT, TOTALLY CONNECTED SECURITY:

- Convergence of Cyber Crime, Organized Crime and Terrorism
  - discussed current challenges faced by law enforcement
  - identification theft is prevalent
- To adapt, we need to mirror what terrorists are doing. Must consider:
  - expertise
  - outsourcing
  - training
  - multi-disciplinary approach
- Need a proactive rather than a reactive approach

DAY 2 OF 4TH ANNUAL INTERNATIONAL CONFERENCE ON PUBLIC SAFETY: TECHNOLOGY AND COUNTER-TERRORISM:
15 March 2005

R. DAVID HENZE, BUSINESS DEVELOPMENT EXECUTIVE, IBM GLOBAL SERVICES, rdhenze@us.ibm.com

- "Technology is moving so fast, that before it is in front of a legislative panel . . . technological threats have already been breached."
- "Cyber-terrorism is just waiting to happen"
- Privacy and anonymity have a cost
- Business requirements: security through strong authentication is needed, as are security identification management
- Secure identification management:
    - to identify information users
    - to secure policies
    - applications, etc, all need to be in place

DAY 2 OF 4TH ANNUAL INTERNATIONAL CONFERENCE ON PUBLIC SAFETY: TECHNOLOGY AND COUNTER-TERRORISM:
15 March 2005

STEPHEN FLYNN, HOMELAND SECURITY EXPERT, FORMER U.S. COAST GUARD:

- Urgency and threat to homeland security
  - "we cannot rest on our laurels"
  - "we must be very careful not to oversell what we're achieving
- Framework for new approach
  - 9/11 shows how warfare can be conducted in the 21st century
  - security is not a manhunt with an existing cast of member
  - we must deal with security on a globalized scale
- Pre-9/11 framework:
  - open network of ports
  - based on efficiency
  - reliability
  - and low cost

  → security was not built into networks because it undermines all 4 goals
- Exploitation increases "with WMD and bad intentions to do substantial damage"
- Networks are conduits, vulnerable and worthy of security
- 9/11 changes little of how things are done
  - it's important to look at history
  - we must adapt and adopt a new form of warfare
  - new warfare is catastrophic and directed against non-military
- 20th Century approach to maritime security is insufficient because it focuses on problems "over there" (overseas) and neglects the homeland defense element
- "We domesticated the global challenge . . . by declaring a new threat as homeland security"
  - problem→resources suddenly were all misguided and directed at a domestic problem rather than a global problem
  - there must be "sufficient market incentive for the private sector to protect itself"
  - but there must be funding, because States don't have the $ to do address the threat
  - Two Problems
    - "tragedy of comedies" = no single company owns all the infrastructure and securing piecemeal doesn't do enough. Furthermore, the government does not have all the information
      - consider costs of security measures
      - protection operations are ineffective if you can't get everyone else to go along with it
      - if we acknowledge a threat, we must be careful about addressing it with voluntary means because certain individuals/companies/businesses may be concerned about opening themselves up to liability → if they know of the threat, will their actions be deemed sufficient?

        - if private sector agrees and then we later discover that security measures implemented fail to address the threat (or are circumvented), "politicians will be the first to say that it [security measures] were insufficient and bad"
    - Potential Solution:
        - partner with the public sector
        - address indemnity issues
        - provide Good Samaritan Protection
        - need the government to provide protection beyond pilots, etc.
- Identification must be adequate to provide security against today's threat
    - Problem with "trying to eliminate the adversary by looking for a vaccine"
    - that approach won't provide protection
    - vaccine approach is to "protect the immune system" by making one more resilient, but we're facing a changing and present threat that cannot be eradicated
- Security Measures just about security will fail → such an approach will lead to complacency and breaches in sophisticated security techniques
    - must provide and market for the ongoing needs of the public good
    - a viable approach must provide dual benefits to be sustainable
- Suggested approach
    - add several measures as deterrents
    - don't let breaches lead to disruption intended
    - must bolster immune system while realizing you cannot provide a single fix
    - protect from targeting and exploitation
    - rather than searching for 100% security in logistics and the supply chain, must take low risks and identify what is low risk
    - Possible Solutions:
        - focus less on infrastructure as a conduit and concurrently focus on it as a target
        - gear focus towards managing attacks and increasing likelihood of failures