Best Practice for Sharing Threats and Warning Information Between Industry and the U.S. Government

Presented to the

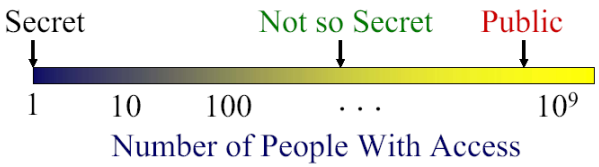
CSIIR Workshop at Oak Ridge National Laboratory

By

Steve Lines

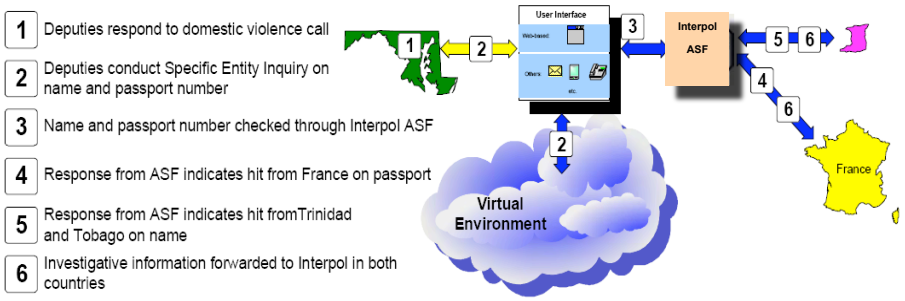
May 13, 2008

Keeping a Secret
(While Sharing Broadly)



Criminals Persist in Evading Capture, Playing the Jurisdictional Game*

Figure 6-3: Domestic Disturbance Leads to Arrest of International Fugitive Wanted For Murder



*Department of Justice (DOJ) Law Enforcement Information Sharing Program

ASF= Automated Search Facility

Criminals Persist in Evading Capture Playing the Jurisdictional Game*

A sheriff's office in Maryland is dispatched to the scene of a domestic disturbance near a public sporting facility. Witnesses identify two persons as involved in the disturbance. As the deputies are questioning the male and female, one of the witnesses informs the deputies that, prior to their arrival, the male hid a duffle bag behind a parked vehicle. The male subject refuses to identify himself and disavows ownership of the duffle bag.

The deputies conduct a Specific Entity Inquiry on the name, date of birth, and passport number. No domestic information is returned. However, the Specific Entity Inquiry also creates an additional inquiry to the Interpol Automated Search Facility (ASF).

The response from the ASF indicates the passport number is a stolen blank taken in an armored car robbery in France, where 9,000 passport blanks were taken. In addition, the name on the passport is listed as an alias on an Interpol Red Notice for murder from Trinidad and Tobago. The response provides a telephone number to call for confirmation. The United States National Central Bureau (USNCB) for Interpol is contacted and is able to retrieve the Red Notice containing a photograph of the suspect as well as the correct name.

The suspect is held on local charges pending the arrival of the Provisional Arrest request from Trinidad and Tobago. The USNCB duty agent notifies the Department of Justice Office of International Affairs and the United States Marshals Service for follow-up. The USNCB duty agent is able to retrieve interview and investigative information from the sheriff's department and forward the information to Interpol France for a follow-up investigation on the armored car robbery and to Interpol Trinidad and Tobago for a follow-up on the murder.

*DOJ Law Enforcement Information Sharing Program

Legal Barriers to Information Sharing

- Restrictions of sharing intel information to law enforcement led to 9/11*
  - Differences in missions, cultures and legal authorities
  - Foreign Intelligence Surveillance Act (FISA) 1978
- Need to share
  - Bremmer's National Commission on Terror 2000

    "Law enforcement agencies are traditionally reluctant to share information outside of their circles so as not to jeopardize any potential prosecution."

*107th U.S. Congress, Select Committee on Intelligence

9/11 Changed the World

Patriot Act, October 2001

"The law allows our intelligence and law enforcement officials to continue to share information. It allows them to continue to use tools against terrorists that they used against -- that they use against drug dealers and other criminals. It will improve our nation's security while we safeguard the civil liberties of our people. The legislation strengthens the Justice Department so it can better detect and disrupt terrorist threats. And the bill gives law enforcement new tools to combat threats to our citizens from international terrorists to local drug dealers."

-- President George W. Bush

Patriot Act Promotes Information Sharing

"*The Patriot Act authorizes vital information sharing to help law enforcement and intelligence officials connect the dots before terrorists strike. The Patriot Act enables necessary cooperation and information sharing by helping to break down legal and bureaucratic walls separating criminal investigators from intelligence officers."*

-- President George W. Bush

Private Industry Issues

Critical Infrastructure Protection Act 2002
HR 5005-12 Title II

(1) To access, receive, and analyze law enforcement information, intelligence information, and other information from agencies of the Federal Government, State and local government agencies (including law enforcement agencies), and private sector entities, and to integrate such information in order to

(A) identify and assess the nature and scope of terrorist threats to the homeland;

(B) detect and identify threats of terrorism against the United States; and

(C) understand such threats in light of actual and potential vulnerabilities of the homeland.

Homeland Security Presidential Directive 7
December 17, 2003

…To the extent permitted by law, Federal departments and agencies with cyber expertise, including but not limited to the Departments of Justice, Commerce, the Treasury, Defense, Energy, and State, and the Central Intelligence Agency, will collaborate with and support the organization in accomplishing its mission. The organization's mission includes analysis, warning, information sharing, vulnerability reduction, mitigation, and aiding national recovery efforts for critical infrastructure information systems…

National Infrastructure Protection Plan (NIPP) 2006

"The effective implementation of the NIPP is predicated on active participation by government and private sector security partners in robust multi-directional information sharing. When owners and operators are provided with a comprehensive picture of threats or hazards to critical infrastructure and key resources and participate in ongoing multi-directional information flow, their ability to assess risks, make prudent security investments, and take protective actions is substantially enhanced."

The National Infrastructure Protection Plan (NIPP) Framework

"Efficient information-sharing and information-protection processes based on mutually beneficial, trusted relationships help to ensure implementation of effective, coordinated, and integrated CI/KR [critical infrastructure and key resources] protective programs and activities…The NIPP uses a network approach to information sharing that represents a fundamental change in how security partners share and protect the information needed to analyze risk and make risk-based decisions. A network approach enables secure, multidirectional information sharing between and across government and industry."

- The NIPP uses the Government Coordinating Council/Sector Coordinating Council (GCC/SCC) model for information sharing.
- The primary functions of an SCC include the following:
  - Represent a primary point of entry for government into the sector for addressing the entire range of CI/KR protection activities and issues for that sector
  - Serve as a strategic communications and coordination mechanism between CI/KR owners, operators, and suppliers, and with the government during response and recovery as determined by the sector
  - Identify, implement, and support the information-sharing capabilities and mechanisms that are most appropriate for the sector. Information Sharing Analysis Centers (ISACs) may perform this role if so designated by the SCC.

DHS Protected Critical Infrastructure Information (PCII) Program 2006

- The Protected Critical Infrastructure Information (PCII) is an information-protection program that enhances information sharing between the private sector and the government. The Department of Homeland Security (DHS) and other federal, state and local analysts use PCII to
  - Analyze and secure critical infrastructure and protected systems
  - Identify vulnerabilities and develop risk assessments
  - Enhance recovery preparedness measures
- If the information submitted satisfies the requirements of the Critical Infrastructure Information Act of 2002, it is protected from
  - The Freedom of Information Act (FOIA)
  - State and local disclosure laws
  - Use in civil litigation
- PCII cannot be used for regulatory purposes and can only be accessed in accordance with strict safeguarding and handling requirements

History of the Network Security Information Exchanges (NSIEs)

"Since the public networks are increasingly driven by software, the NCS should consider how to protect the public networks from penetration by hostile users…"

Growing Vulnerability of the Public Switched Network, 1989
National Research Council

"What actions are required by Government and industry" considering the "current and evolving vulnerabilities of the telecommunications network to the 'hacker' threat?"

National Security Council
Memorandum to the Manager, National Communications System, April 1990

- **The National Communications System (NCS) and the National Security Telecommunications Advisory Committee (NSTAC) identified the need to share information within government and industry, and between government and industry**
- **Government and NSTAC Network Security Information Exchanges (NSIEs) established**
- **First meeting of NSIEs held in June 1991**

History of the Network Security Information Exchanges (NSIEs)

- Working forum to identify issues involving penetration or manipulation of software and databases affecting national security/emergency preparedness telecommunications
- Assesses network risks and acquires threat mitigation information and develops recommendations to reduce network security vulnerabilities
- Shares information with those trying to protect the network as effectively as those interested in attacking the network
- Provides expertise to the National Security Telecommunications Advisory Council (NSTAC) on which to base network security recommendations to the U.S. president
- Trust - non disclosure agreement (NDA) and security clearance
- Government and NSTAC chairs - the National Communications System is champion for the process
- U.S. National Security Information Exchange (NSIE) – ongoing since 1991
- International introduction to the NSIE process
  - UK NSIE – 2003
  - Canadian NSIE – like group – 2005
  - 2007 Trilateral NSIE meeting, Abingdon, UK – March 2007
  - 2008 Trilateral NSIE meeting, Banff, Canada – June 2008

Membership in NSIE

Government NSIE Members

Central Intelligence Agency
Department of Justice
Defense Intelligence Agency
Department of Defense
- Defense Intelligence Agency
- JTF-GNO
- OSD/NII
- USNORTHCOM
- USSTRATCOM

Department of Justice
- Federal Bureau of Investigation

Department of Homeland Security
- NCS/NCC/ISAC
- NCSD/US-CERT
- U.S. Secret Service

National Institute of Standards & Technology
National Security Agency

NSTAC NSIE Members

AT&T
AT&T Wireless
Bank of America
Boeing
Cisco
CSC
Juniper Networks
Lockheed Martin
Lucent Technologies
Nortel
Northrop Grumman
Qwest
Raytheon
SAIC
Sprint Nextel
Telcordia
Verizon
Verizon Business
Verizon Wireless

NSIE Reach into Related Communities

UK NSIE
Canadian NSIE
Intelligence Community
National Intelligence Estimate Process
Law Enforcement Community
Electronic Crimes Task Force
InfraGard
FIRST
Other ISACs, incl. Financial Services
CERT Community
National Information Assurance Partnership (NIAP)

Other Members, Including International

British Telecom (BT)
CERT/CC
Industry Canada
UK NSIE
Canadian NSIE

Information exchange occurs not only among government and NSTAC NSIE representatives but extends beyond the membership to other entities

DSIE and the DoD

- The Defense Security Information Exchange (DSIE) is the information sharing organization for the Defense Industrial Base Sector Coordinating Council (DIB SCC) to collectively share cyber threat and warning information between members of the DIB SCC
- Sector Coordinating Council/Government Coordinating Council structure integrated approach
- Two separate organizations, one DoD and one industry, again models the two National Security Information Exchange organizations
- Information sharing should be on two levels:
  - Strategic (higher level, policy issues)
  - Tactical (near real-time threat and warning sharing)

Operating Principals

- The Defense Security Information Exchange (DSIE) is the Cyber Security Sub Council of the Defense Industrial Base Critical Infrastructure Protection Sector Coordinating Council (DIB CIP SCC).
- The DSIE is a sub committee of the National Defense Industrial Association (NDIA). Membership is limited to members of the NDIA as the strategic committee.
- This strategic committee of the DSIE will work with the DIB CIP SCC on policy issues with the DSIE and the DoD in their pilot program for information sharing (DoD-DIB Collaborative Information Sharing Environment, DCISE).
- There will be a larger tactical information sharing group that will interface within the DSIE. Membership would be vetted by the strategic committee.

Membership in the DIB SCC

- Open to any existing industry association member predominately representing significant defense industrial base business interests. "Core" member associations include
  - Aerospace Industries Association (AIA)
  - American Society for Industrial Security (ASIS)
  - Industrial Security Working Group (ISWG)
  - National Classification Management Society (NCMS)
  - National Defense Industrial Association (NDIA)
- Council members must possess an authoritative knowledge of defense industrial base industrial capabilities and infrastructure protection requirements

Membership (cont)

Current members of the Defense Security Information Exchange include

SAIC	General Atomic
Lockheed Martin	Rolls Royce
Boeing	Pratt-Whitney
Raytheon	BAE Systems
GD	Honeywell
Northrop Grumman	Rockwell Collins
BAH	Orbital
General Dynamics	AAI Corp
General Electric	ATK
L3	MITRE

Corporate Members to Date in the DIB CIP SCC**

Alliant Techsystems
BAE Systems*
Boeing Company*
Computer Sciences Corporation
General Dynamics*
L3-Communications*
Lockheed Martin Corporation*
Mantech International
Northrop Grumman Corporation*
Raytheon Company*
Science Applications International Corporation *
Washington Group International

*Those starred are in the Defense Security Information Exchange
**Defense Industrial Base Critical Infrastructure Protection Sector Coordinating Council

Operating Principles

The operating principles of the Defense Security Information Exchange (DSIE) are as follows:

- Due to the sensitive nature of the information that may be discussed at DSIE meetings,
  - attendance will be limited to member representatives and guests invited with the prior approval of the Chairs; and,
  - recording devices of any kind will not be permitted at DSIE meetings unless specifically authorized by the group.
- All member organizations, their representatives and their guests must sign a nondisclosure agreement before attending their first meeting.
- DSIE will share information using the Critical Information Partnership Advisory Council mechanism as identified in the National Infrastructure Protection Plan.
- All representatives must have, or be capable of acquiring upon appointment, a security clearance at the SECRET level or higher.

Operating Principles, (con't)

- Summary meeting notes will be prepared, marked FOUO/proprietary/classified as required by the content, and limited in distribution.
- The strategic committee shall meet jointly on a bi-monthly basis to exchange information on threats, vulnerabilities, remedies, and risks.
- Whenever possible, within the constraints of the Nondisclosure Agreement, the Defense Security Information Exchange will share information with other organizations through workshops, symposiums, and similar activities.
- Members of the group will be able to post advisories to other members of the group in real time on suspected threats to their infrastructure in a non-repudiated manner. As such we are working with the Homeland Security Information Network portal. Current members have been invited to join. Other options are being explored. These advisories would be considered confidential business information, therefore not publicly releasable under the Freedom of Information Act.

Summary of Information Sharing Organizations

- DoD
  - NII Cyber Task Force
  - Government Coordinating Council
  - 8th Air Force Cyber Command
  - Navy Cyber Defense Operations Command (NETWARCOM)
  - Army Cyber Command
  - Defense Cyber Crime Center (DC3)
  - Defense Critical Infrastructure Program (DCIP)
- DHS and the National Infrastructure Protection Plan
  - Sector Coordinating Councils (SCC)
  - Critical Information Partnership Advisory Council (CIPAC)
    - Defense Security Information Exchange (DSIE)
    - DoD-DIB Collaborative Information Sharing Environment (DCISE) Headed by DC3
  - Information Sharing Analysis Centers (ISAC)
  - National Security Telecommunications Advisory Council (NSTAC)
    - Network Security Information Exchange (NSIE)
  - Office of the Protected Critical Infrastructure Information (PCII)
- FBI
  - Infragard
  - Domain
- USSS
  - Electronic Crimes Task Force

Summary of Information Sharing Organizations (more)

- Global Justice Information Sharing Initiative
- National Criminal Intelligence Sharing Plan
- Markle Foundation Task Force: Creating A Trusted Network For Homeland Security
- 9/11 Commission Report and Recommendations
- Law Enforcement Regional Data Exchange
- Intelligence Community Information Sharing Working Group
- Community Interoperability and Information Sharing Office Policy Board
- DOJ-DHS Ad Hoc Working Group on SBU-level Information Sharing Systems
- National Virtual Pointer System Coordinating Committee
- Justice Intelligence Coordinating Council
- Homeland Security Advisory Council Working Group
- National Association of State Chief Information Officers
- Joint Terrorism Task Force
- Etc, Etc, Etc

Office of the Secretary of Defense

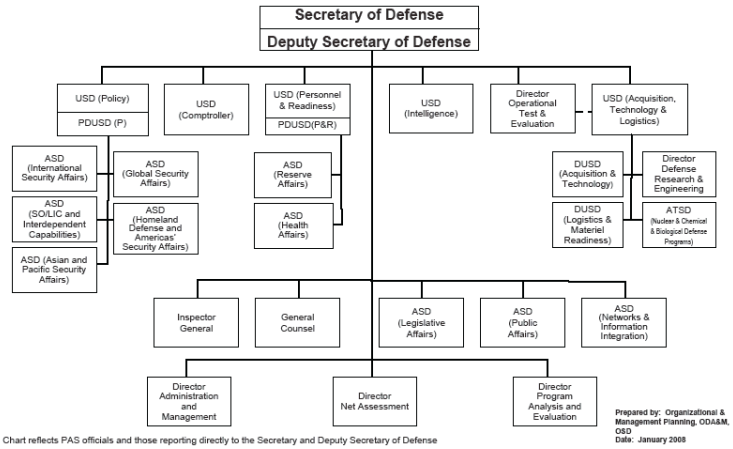


Chart reflects PAS officials and those reporting directly to the Secretary and Deputy Secretary of Defense

Why can't we all just get along? Barriers to Information Sharing

These include:

- **Trust**
  - Let's share our most embarrassing moments…You first!
- **Information is power**
- **Culture differences**
- **Legal barriers**
- **Classified programs**
  - Need to know vs. need to share
- **Liability issues**
- **Contractual obligations**
- **Stockholder value**

What Are the Bad Guys Doing?

- ShadowServer.org
  - 1,600 botnets monitored on a daily basis
  - Some 10,000 computers, some > 250,000
  - They talk to each other every day!

The New China Syndrome

- *Time* magazine, August 5, 2005
  - Titan Rain ("Inside the Chinese Hack Attack")
- *BusinessWeek* reports, April 10 2008
  - Operation Byzantine Foothold (Chinese infiltrate private industry)
- Russian Business Network (RBN)
  - Pornography
  - Extortion
  - Host >60% of world's cyber criminals
    - Resale of personal identities
    - Botnets
    - Fake downloads to install malicious software

Attacks are becoming much more sophisticated as the stakes rise!

Fake Russian Business Network Download

Information Sharing

"The Federal Government needs to establish policies and processes for sharing terrorism-related and sensitive but unclassified information."

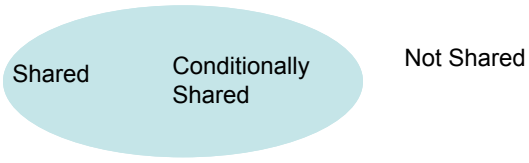
United States Government Accountability Office
Report to Congressional Requesters (GAO-06-385)
March 2006

NIPP Implementation Actions

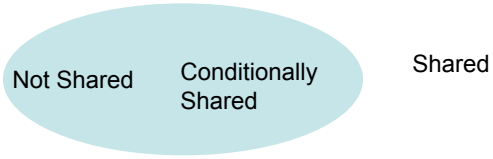
The effective implementation of the National Infrastructure Protection Plan (NIPP) is predicated on active participation by government and private sector security partners in robust multi-directional information sharing. When owners and operators are provided with a comprehensive picture of threats or hazards to critical infrastructure and key resources and participate in ongoing multi-directional information flow, their ability to assess risks, make prudent security investments, and take protective actions is substantially enhanced.

NIPP implementation will rely greatly on critical infrastructure information provided by the private sector. Much of this is sensitive business or security information that could cause serious damage to companies, the economy, and public safety or security through unauthorized disclosure or access to this information.

Information Sharing Environment, Today



Information Sharing Environment Goal



Contact Information

Steve Lines, CISSP, CISM, CISA, IAM
Director of BCP and Information Assurance
SAIC
6723 Odyssey Dr.
Huntsville, Alabama 35757
Office: 256-971-6696
Steven.R.Lines@saic.com