2008 Defense Industrial Base – Critical Infrastructure Protection Conference (DIB-CBIP)

Miami, FL

7-9 April 2008

Agenda

Tuesday, April 8

DOD Keynote Address- DOD Support to Preparedness & Response
Mr. Peter F. Verga, Principal Deputy Assistant Secretary of Defense, Homeland Defense and Americas’ Security Affairs

Cyber Security and Information Assurance
Lieutenant General Robert J. Elder, USAF, Joint Functional Component Commander for Global Strike and Integration, U.S. Strategic Command

“The Business of Vulnerabilities- How Economics is Driving Cyber Threats to Infrastructure”
Mr. Aaron Turner, Cyber Security Strategist, Idaho National Laboratory

“Cyber Security Overview & Update…The State of U.S. Cyber Security” Mr. Richard Hale, Chief Information Assurance Executive, DISA

Panel- Cyber Security; Industry and Government Best Practices
Moderator: Mr. Rick Anderson, Deputy Director, Defense Industrial Base Cyber Security Task Force
Panel:

Supply Chain/Response Management
Mr. John Rank, Vice President, Supply Chain, General Dynamics

Wednesday, April 9

Intelligence & Threat Warning; Opportunities For Public/Private Partnerships
Mr. Ronald T. “Rudy” Guerin, Executive Vice President, Pamir Resources & Consulting, Inc.

Panel – Improving the Sharing and Reliability of Public and Private Threat and Hazard Information
Moderator: Mr. Steve Lines, Director, Information Assurance, SAIC
Monday, April 7

2:00pm - 5:00pm  CIPAC Meeting (Invitation Only)
5:00pm - 6:30pm  DIB CIP Exhibits Open
5:00pm - 6:30pm  Registration and Reception (Cash Bar)

Tuesday, April 8

7:00am - 8:00am  Registration and Continental Breakfast
8:00am  Welcoming Remarks
         MG Barry D. Bates, USA (Ret), Vice President-Operations, NDIA
8:15am  Conference Overview and Objectives
         Mr. Antwane Johnson, Director, Critical Infrastructure Protection, OASD (HD&ASA)
8:30am  DOD Keynote Address- DOD Support to Preparedness & Response
         Mr. Peter F. Verga, Principal Deputy Assistant Secretary of Defense, Homeland Defense and Americas’ Security Affairs
9:15am  Cyber Security and Information Assurance
         Lieutenant General Robert J. Elder, USAF, Joint Functional Component Commander for Global Strike and Integration, U.S. Strategic Command
10:00am  Break in Exhibits Area
10:00am - 6:00pm  Exhibits Open
10:15am  “The Business of Vulnerabilities- How Economics is Driving Cyber Threats to Infrastructure”
          Mr. Aaron Turner, Cyber Security Strategist, Idaho National Laboratory
10:45am  “Cyber Security Overview & Update…The State of U.S. Cyber Security”
          Mr. Richard Hale, Chief Information Assurance Executive, DISA
11:30am  Panel- Cyber Security; Industry and Government Best Practices
          Moderator: Mr. Rick Anderson, Deputy Director, Defense Industrial Base Cyber Security Task Force

Panel:
- Mr. Jerry Cochran, Principal Security Strategist, Trustworthy Computing/CIP, Microsoft Corporation
- Mr. Tommy Augustsson, Vice President, Information Technology, General Dynamics Corporation
- Mr. Richard Hale, Chief Information Assurance Executive, DISA
- Dr. Mark Thomas, Senior Advisor, Defense Industrial Base Task Force
12:30pm  Lunch
2:00pm  Supply Chain/Response Management
Mr. John Rank, Vice President, Supply Chain, General Dynamics
2:45pm  Break in Exhibits Area
3:00pm  Panel- Supply Chain/RM; Global Supply Chain Vulnerability and Security Issues
Moderator: Robert Connors, CBCP, MBCI, Director, Preparedness, Raytheon Company
Panel:
- Mr. William Osborne, Director, Engineering and Network Systems, General Dynamics Corporation
- Mr. Gene Tyndall, President, Supply Chain Executive Advisors
- Mr. Caleb Jones, Assistant Vice president, Risk Management, Alion Science and Technology
- Mr. Sydney Pope, Industrial Policy Advocate, Electronic Systems and Information Technologies, ODUSD (Industrial Policy)
4:00pm  Session Wrap-up and Closing Remarks
4:30pm - 6:00pm  Hosted Reception in the Exhibits Area

Wednesday, April 9

7:00am - 8:00am  Registration and Continental Breakfast
8:00am  Welcoming Remarks
MG Barry D. Bates, USA (Ret), Vice President-Operations, NDIA
8:15am  Industry Keynote Address - A Corporate-Wide View to Security and Business Continuity
Mr. Stephen Colo, Senior Vice President and Chief Security Officer, SAIC
9:00am  Intelligence & Threat Warning: Combating the Insider Threat (Physical, Personnel, Procedural and Information Systems)
Lieutenant General Patrick Hughes, USA (Ret), Vice President Intelligence and Counterintelligence, L3-Communications
9:45am  Break in Exhibits Area
9:45am - 2:20pm  Exhibits Open
10:15am  Intelligence & Threat Warning: Opportunities For Public/Private Partnerships
Mr. Ronald T. “Rudy” Guerin, Executive Vice President, Pamir Resources & Consulting, Inc.
11:00am  Panel – Improving the Sharing and Reliability of Public and Private Threat and Hazard Information
Moderator: Mr. Steve Lines, Director, Information Assurance, SAIC

Panel:

- Mr. Ray Musser, Director, Corporate Security, General Dynamics Corporation
- Special Agent Chuck Frahm, Deputy Assistant Director, FBI
- Mr. Vince Jarvie, Vice-President, Corporate Security, L-3 Communications
- Mr. Steve Shirley, Executive Director, Defense Cyber Crime Center (DC3)

12:15pm Lunch Presentation
Mr. Robert Stephan, Assistant Secretary for Infrastructure Protection, DHS

2:15pm Session Wrap-up and Closing Remarks
MG Barry D. Bates, USA (Ret), Vice President -Operations, NDIA

2:20pm Conference Wrap up
Mr. Peter F. Verga, Principal Deputy Assistant Secretary of Defense, Homeland Defense and Americas’ Security Affairs
A variety of actors threaten the security of our cyber infrastructure. Terrorists increasingly exploit the Internet to communicate, proselytize, recruit, raise funds, and conduct training and operational planning. Hostile foreign governments have the technical and financial resources to support advanced network exploitation and launch attacks on the informational and physical elements of our cyber infrastructure.

In order to secure our cyber infrastructure against these man-made and natural threats, our Federal, State, and local governments, along with the private sector, are working together to prevent damage to, and the unauthorized use and exploitation of, our cyber systems.
Cyber Security; Government and Industry
Best Practices Panel Members

Dr. Tommy Augustsson, CIO  General Dynamics, taugusts@generaldynamics.com, 703-876-3473

Mr. Jerry Cochran, Principal Security Strategist, Microsoft Jerry.Cochran@microsoft.com

Mr. Richard Hale, Chief Information Assurance Executive, DISA Richard.hale@disa.mil  703-882-1500

Dr. Mark Thomas, Senior Advisor, Army DIB Task Force Mark.Thomas2@us.army.mil  703-697-9424

Mr. L. Rick Anderson, Dep, Dir DIB Cyber Security Task Force Levon.Anderson@osd.mil  703-604-5523, ext 123
What are some of the major partnership challenges between DOD and Industry as related to cyber security info sharing and reporting? Provide possible or proven solutions if applicable (e.g., technology, procedural, regulatory, etc...).
Cyber Domain Protection and the National Defense

NDIA Defense CIP Conference 2008

Lt Gen Bob Elder
8 April 2008
THREATS

“… today, when individuals can easily access all the tools of collaboration and superempower themselves, or their small cells, individuals do not need to control a country to threaten large numbers of people.”

OPPORTUNITIES

“We need to think more seriously than ever about how we encourage people to focus on productive outcomes that advance and unite civilization.”

From The World is Flat, Thomas L. Friedman
“IMAGINE that agents of a hostile power, working in conjunction with organised crime, could ... paralyse business, the media, government and public services, and cut you off from the world. That would be seen as a grave risk to national security, surely?”

- Peter Schrank, on Estonia in “The Economist,” May 07
Increased Commercial Use of Cyber

- Communication & Information Sharing
- Social Networking
- Production Controls
- Education and Creativity
- Productivity Enhancement
- Navigation
- e-Commerce (and e-Barter)
- Banking & Finance
- Entertainment

Lessons from 9-11, Hurricane Katrina:

We are increasingly dependent on cyber use for business, public safety, and daily life
### Cyber Criminal Activities

<table>
<thead>
<tr>
<th>Rank</th>
<th>Item</th>
<th>Percentage</th>
<th>Price Range</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Credit Cards</td>
<td>22%</td>
<td>$0.50-$5</td>
</tr>
<tr>
<td>2</td>
<td>Bank Accounts</td>
<td>21%</td>
<td>$30-$400</td>
</tr>
<tr>
<td>3</td>
<td>E-mail Passwords</td>
<td>8%</td>
<td>$1-$390</td>
</tr>
<tr>
<td>4</td>
<td>Mailers</td>
<td>8%</td>
<td>$8-$10</td>
</tr>
<tr>
<td>5</td>
<td>E-mail Addresses</td>
<td>6%</td>
<td>$2/MB-$4/MB</td>
</tr>
<tr>
<td>6</td>
<td>Proxies</td>
<td>6%</td>
<td>$0.50-$3</td>
</tr>
<tr>
<td>7</td>
<td>Full Identity</td>
<td>6%</td>
<td>$10-$150</td>
</tr>
<tr>
<td>8</td>
<td>Scams</td>
<td>6%</td>
<td>$10/week</td>
</tr>
<tr>
<td>9</td>
<td>Social Security Numbers</td>
<td>3%</td>
<td>$5-$7</td>
</tr>
<tr>
<td>10</td>
<td>Compromised Unix Shells</td>
<td>2%</td>
<td>$2-$10</td>
</tr>
</tbody>
</table>

Breakdown of goods available on underground economy servers
Source: Symantec Corporation, Sep 2007
## Sources of Malicious Activity

<table>
<thead>
<tr>
<th>Overall Rank</th>
<th>Country</th>
<th>Overall Proportion</th>
<th>Malicious Code Rank</th>
<th>Spam Zombie</th>
<th>Cmd&amp;Ctrl Server Rank</th>
<th>Phishing Websites</th>
<th>Bot Rank</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>USA</td>
<td>30%</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>2</td>
<td>China</td>
<td>10%</td>
<td>2</td>
<td>3</td>
<td>5</td>
<td>18</td>
<td>1</td>
</tr>
<tr>
<td>3</td>
<td>Germany</td>
<td>7%</td>
<td>7</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td>4</td>
<td>UK</td>
<td>4%</td>
<td>3</td>
<td>15</td>
<td>6</td>
<td>3</td>
<td>7</td>
</tr>
<tr>
<td>5</td>
<td>France</td>
<td>4%</td>
<td>9</td>
<td>7</td>
<td>12</td>
<td>6</td>
<td>5</td>
</tr>
<tr>
<td>6</td>
<td>Canada</td>
<td>4%</td>
<td>6</td>
<td>31</td>
<td>3</td>
<td>7</td>
<td>8</td>
</tr>
<tr>
<td>7</td>
<td>Spain</td>
<td>3%</td>
<td>10</td>
<td>10</td>
<td>22</td>
<td>13</td>
<td>4</td>
</tr>
<tr>
<td>8</td>
<td>Italy</td>
<td>3%</td>
<td>5</td>
<td>6</td>
<td>8</td>
<td>12</td>
<td>6</td>
</tr>
<tr>
<td>9</td>
<td>S. Korea</td>
<td>3%</td>
<td>26</td>
<td>8</td>
<td>4</td>
<td>10</td>
<td>13</td>
</tr>
<tr>
<td>10</td>
<td>Japan</td>
<td>2%</td>
<td>4</td>
<td>20</td>
<td>13</td>
<td>8</td>
<td>16</td>
</tr>
</tbody>
</table>

**Malicious Activity by Country**

*Source: Symantec Corporation, Sep 2007*
Growing Dependence on Electromagnetic Spectrum

1975 Frequency Allocation Chart

2007 Frequency Allocation Chart

Fly - Fight - Win
"Espionage used to be a problem for the FBI, CIA and military, but now it's a problem for corporations," Brenner said. "It's no longer a cloak-and-dagger thing. It's about computer architecture and the soundness of electronic systems."

Joel Brenner, ODNI Counterintelligence Office

As reported in “Espionage Network Said to Be Growing”
Washington Post, 3 April 2008
Cyber will continue to be a contested environment.

The infrastructure on which the Air Force depends is controlled by both military and commercial entities and is vulnerable to attacks and manipulation.

Operations in the cyber domain have the ability to impact operations in other war-fighting domains.

Air Force must maintain capability to operate when the reception, processing, and distribution of vital information is challenged.

Nation must defend against data manipulation and denial of service; it’s not just an issue of data theft.
The Mission of the United States Air Force is to provide sovereign options for the defense of the US and its global interests—to fly and fight in air, space, and cyberspace.
Cyberspace is a domain with characteristics comparable to the air, space, and maritime domains.
Cyber ops require global and theater integration across all domains.

Cyberspace crosses all the domains.
# Cyber Domain Exploitation

<table>
<thead>
<tr>
<th>Government Activities</th>
<th>Admin &amp; Logistics</th>
</tr>
</thead>
<tbody>
<tr>
<td>Military Operations</td>
<td>Health Services</td>
</tr>
<tr>
<td>Intelligence Collection</td>
<td>Sales &amp; Marketing</td>
</tr>
<tr>
<td>Banking &amp; Finance</td>
<td>Education</td>
</tr>
<tr>
<td>Police &amp; Security</td>
<td>Social Networking</td>
</tr>
<tr>
<td>Utility Management</td>
<td>Information Management</td>
</tr>
<tr>
<td>Terrorist Activities</td>
<td>Knowledge Management</td>
</tr>
<tr>
<td>Criminal Activities</td>
<td>Entertainment</td>
</tr>
</tbody>
</table>
Cyber Ops Planning “Terrain” Map

United States and friendly Cyber elements

Global Information Grid and DOD Networks

US Government

US Cyberspace

US Interests in Cyberspace

Other Cyberspace & Associated Cyber Infrastructure

Adversary-owned Cyber Networks

Adversary Military Cyber Networks

Adversary Cyber elements
The National Strategy to Secure Cyberspace (DHS lead)

- Establish a **public-private architecture** for national response
- Provide for the development of tactical and strategic analysis of cyber attacks and vulnerability assessments
- Encourage the development of a **private sector capability** to share a synoptic view of the health of cyberspace
- Expand the Cyber Warning and Information Network to support DHS cyberspace crisis management
- Improve national incident management
- Coordinate voluntary participation in national public-private continuity and contingency plans
- Exercise cyber security continuity plans for federal systems
- Improve and enhance **public-private information sharing** involving cyber attacks, threats, and vulnerabilities
AF Cyber Support: Civil Authorities

- JTF-GNO (STRATCOM)
- NORTHCOM (1 AF)
- 8AF (AFCYBER)
- Intelligence Community
- Law Enforcement
- Homeland Security Spt Centers
- Research Community
- JTF-GNO Service Components
Cyber Support: Defense Industry

- DIB IA TF (& DC3)
- Defense Industry
- Law Enforcement (AFOSI)
- NAVNETWARCOM
- Army NETCOM
- JTF-GNO
- Cyber Research Centers
- Intelligence Community
- 8 AF (AFCYBER)
- Acquisition Program Offices

Fly - Fight - Win
National Military Strategy for Cyberspace Ops (NMS-CO)

Ways:
- Information Operations
- Network Operations
- Kinetic Actions
- Law Enforcement
- Counter-intelligence

Enablers:
- Science & Technology
- Partnering
- Intelligence Support
- Law and policy
- Trained personnel

Joint Capability Areas:
- Battlespace Awareness
- Force Generation
- Command and Control
- Information Operations
- Net-centric Operations
- Global Deterrence
- Homeland Defense
- Interagency Integration
- Non-governmental organization coordination

Fly - Fight - Win
“Fly & Fight” in Cyberspace

Cyber Ops

- Establish the Domain
  - Expeditionary Cyber Ops
  - Cyber Network Ops
- Control the Domain
  - Defense
  - Offense
- Use the Domain
  - Integrated Attack
  - Force Enhancement
  - Support

Cyberspace is a **Warfighting** Domain

14-Apr-08
Control the Cyber Domain

Cyber Effects:
- Denial of Service
- Confidential Data Loss
- Data Manipulation
- System Integrity Loss

Electromagnetic Spectrum Attack
Digital Attack
Logical Networks
Wireless Networks
Electronics (& Infrastructure)

Influence Attack
Electronic Protection
Electromagnetic Spectrum
Data/Code Protection
Digital Data

Social Networks

Cyber Use

Force Protection
Physical Networks
Physical Attack (includes Directed Energy)
Cyber Domain Protection

Mission Assurance

Infrastructure Protection
Electronic Protection
Supply Chain Controls

Perceptions
USER (Social)
Network

Knowledge

Data
Information Assurance

Encapsulation
Logical (Virtual) Network

System Code

Electromagnetic Environment

Electronics

Physical Network

Fly - Fight - Win
Cyber Deterrence

Impose Cost
(Attack Attribution)

Deny Benefits
(Mission Assurance)

Force Posturing
Demonstrate Readiness

Visible Activities
Demonstrate Capabilities

Messaging
Explain Actions

Encourage Restraint
(Identify Actions & Behaviors to Deter)
Challenges and Opportunities

**Challenges**
- Increased cyber dependence
- Supply chain vulnerabilities
- Infrastructure vulnerabilities
- Electronics vulnerabilities
- Sensor disruption & spoofing
- Increased wireless use
- More complex attack vectors
- Growth in cyber crime
- Encryption vulnerabilities

**Opportunities**
- Mission Assurance
- Attack Attribution
- Malware behavior detection
- Altered data/code detection
- Denial of service protection
- Cyber deterrence strategies
- Insider “threat” detection
- Wireless privacy systems
- Intrusion detection/intrusion prevention (IDS/IPS) systems
Assess and characterize cyber protection systems used by the U.S. defense industrial base and their potential impacts to Air Force operations.

Assess and characterize current Air Force operational readiness levels for rapid detection, assessment and response, including the ability to “fight through” a cyber attack and to quickly re-organize networks.

Identify high leverage technology options for generating and maintaining operational readiness, including training, in a variety of scenarios.

Explore the impacts of a layered defense and examine potential new constructs for creating and implementing new network and system architectures, for example, a “demilitarized zone (DMZ)” between the Department of Defense and external customers.

Evaluate the effectiveness of such technology options and recommend near-term and mid-term options for implementation.
Summary: Cyber Domain Protection

- Cyber is a domain ... not just computer networks
  - Co-exists with air, space, land, and sea domains
- Cyber **critical to military operations** and commerce
  - Foundation of the world’s global economy
- Cyber domain elements are under attack today
  - Military vulnerable to direct and indirect attacks
- Global cyber dominance requires new competencies
  - Cyber **Weapon Systems** and Cyber operators
  - **Partnerships** (academia, industry, government)
- Opportunity to deter cyber attacks of mass effects
  - Enabled by **attack attribution & mission assurance**
INTELLIGENCE AND THREAT WARNING
“THE THREAT IS CORPORATE AMERICA”

IT IS ASYMMETRIC WARFARE
“Entities from 108 countries were involved in collection efforts against sensitive and protected US technologies in FY 2005”

- Office of the National Counterintelligence Executive
According to the FBI:

Foreign entities most responsible for Economic Espionage investigations within the US:

- 1. China
- 2. India
- 3. France
- 4. Russia
- 5. Israel
These countries are allowed to utilize their intelligence services to support commercial gain within their own country.

All in the name of national security and economic gain.
“American organizations must begin policing their operations more aggressively today to prevent valuable data from being stolen”

- Info World Magazine 9/14/07
FBI’s DOMAIN PROGRAM

- Tasked to protect US companies sensitive information and technologies
- Corporate America is part of US national security
- Partner FBI with corporate America to identify what is at risk
- Develop plan to protect it
- Build relationships
FBI’S DOMAIN PROGRAM

- Business Alliance

- Academic Alliance

- Protect technology while in the R&D stages
• Technology monitoring developed by Pamir and its partner
• Identified US technologies that were proliferated by foreign entities
• Looks at patent information within 120 countries
• Prevention tool against Insider Threat as well
PREVENTION PROGRAM

- From pre-employment to post-employment
- Proper prevention can diminish loss of technology, number of investigations
- Cannot just react, need to prevent
- (Request of DoJ)
The importance of conducting proper Due Diligence (DD) in an emerging overseas market prior to conducting business overseas cannot be overstated.

- The need to conduct DD as you continue to conduct business in foreign markets.
A Due Diligence (DD) in an emerging market should include:

- Company profile
- Annual inspection
- Any modification on Registration
- Ownership
- Shareholders
- Executives
DUE DILIGENCE

- Investment/Affiliated enterprises
- Banking information
- Loan information
- Balance sheet
- Financial analysis
- Main operation and products
- Suppliers/customers
• Criminal record (national police checks not possible in India)
• Intelligence or military affiliation
• Political or Party affiliation
• China specific: a China context analysis of what it all means
• CAUTION: Be careful to what DD vendors claim regarding the extent of their capabilities
CI AWARENESS PROGRAM

- Need to establish a counterintelligence awareness program that reaches all employees
- Need force multipliers (eyes/ears)
- Need sources
- Need to instill in employees that CI awareness is everyone’s responsibility
- How to report and to whom
- Cyber responsibility
When prevention and monitoring are not enough of a deterrent
Prosecution becomes a priority because of what is at stake
CHI Mak case
DOJ Task Forces
Force multipliers
Build relationships
RUDY GUERIN
PRINCIPAL
100 EAST STREET S.E. SUITE 203
VIENNA, VA 22180
703-319-9646 (O)
703-319-8205 (F)
703-303-9047 (M)
Cyber Security, Information Assurance

Richard Hale
Chief Information Assurance Executive
Defense Information Systems Agency
April 8, 2008
Bad Guys
Bad Guy Motivation:

Gain Military Advantage by…
Knowing what we’re going to do or what we’re likely to do

Slowing our decision cycle

Making our weapons work in unexpected ways

Fuzzing up our view of reality
  – By changing information
  – By participating directly in our decisions (by masquerading as us)

Causing us to lose faith in each other

Etc.
Sophisticated Adversaries
aka *Really Capable Bad Guys*

- Have a military or intelligence mission in mind
- Will plan and select the plan with the best combination of effectiveness, (low) risk to the adversary, and cost
- Are very patient, analytical, methodical, and quiet
- Have advanced resources and tradecraft
- Can select the attack method, the target, the time, and the place
What’s Our Business?

...Twin Goals for Cyber Security/Information Assurance
1. Ensuring that our customers can depend on information and on the information infrastructure in the face of physical and cyber attack

(Mission Assurance, or, we’re all really dependability experts)
2. Ensuring that our customers can keep a secret (when they want to)

... and doing both while sharing as broadly as possible
Keeping a Secret
(While Sharing Broadly)

Number of People With Access

Secret 1 10 100 . . . $10^9$
Not so Secret
Public

$10^9$
My Customers

Anyone in DoD, and anyone involved in a mission important to DoD

We often don’t know in advance with whom DoD will be working
My Oversimplification of How DoD Is Pursuing These IA (and sharing) Goals
Part 1

Limit exposure of vulnerabilities by

– *Removing* as many of these vulnerabilities as possible (e.g. encrypt when appropriate, configure things securely, remove unnecessary functions, eliminate passwords)

– *Layering protections* that incrementally limit the population with access to a given vulnerability (defense-in-depth)

– *Designing* what DoD looks like to partners, to the public, to adversaries
Part 2

**Drive-out anonymity** (and enable net-centricity and improve sharing) by broad use of non-spoofable cyber identity credentials (aka *PKI*)

– Minimize whole classes of worries; brings accountability, *worries some classes of bad guys*

Build and operate an **attack detection and diagnosis** capability that allows rapid, sure, militarily useful reaction to cyber attacks

**Improve joint, coalition, interagency, & industry partner cyber operations/NETOPS** so the above is possible
The Basics: Secure Configuration

(Or...configuring everything securely, keeping everything configured securely, and ensuring the right people know this is so, or not so)
1. Define: Configuration guides with NSA, NIST, industry, military services, DISA

2. Buy it pre-configured

3. Configure it  (Automate)

4. Measure it  (Automate)

5. Change it  (Automate)

6. Report it  (Automate)

Big win: (NSA/NIST/AF/DHS/DISA/Microsoft/OMB): Federal Desktop Core Configuration
Security Content Automation Protocol

**SCAP**

- Name for family of cyber security data standards
  - Configuration description
  - Configuration measurement
  - Vulnerability
  - Etc.

- **NIST in the lead in defining; many are used now**

- **Goals is to improve sharing and improve automation**
  - Ex. “STIG” content can be machine readable and consumed by any compliant tool
  - DoD can purchase automation tools from any vendor that complies
Information Sharing in the Federal Government

Or, *What System-High Wrought*
Sharing With Allies
Q. Does all of this stuff really require system-high separation?

A. (My theory, although many others have concluded the same thing.)

Nope. Some of these networks can be treated as separate communities within a single network infrastructure.

The CCER. The JCS & COCOMs & NII have asked DISA & NSA, to develop and deploy a method of consolidating several of the large CENTRIXS
- CENTRIXS cross enclave requirement (or CCER)
Sharing in the Interagency
New Federal Interconnect net?

Federal, State, & Local Classified Net?

Federal Classified Net

CENTRIXS 1

CENTRIXS 2

CFBLnet

Bi-lat

centrix

SIPRNET

JWICS

NIPRNET

NATO

Internet
A Typical Netcentric Mission Thread

(or, sharing in spite of system high)
How Exactly Does *That* Sharing Work?
Sharing Part 1: That’s What We Do With All That *Cross Domain* Stuff
The Unified Cross Domain Management Office

- Intelligence Community and DoD effort to manage cross domain efforts
  - Approve standard products
  - Help customers find existing or modifiable technologies before developing more
  - Oversee the provision of cross-domain as a network service
  - Monitor technology development
  - Improve MLS certification and accreditation process
    • As part of overall IC/DoD C&A re-engineering
Sharing Part 2: Better DMZs Between DoD and Non-DoD
DoD DMZs

- Internal Servers
- User Workstations
- Publicly Visible Servers in DMZ
- Firewalls With Tight, Customized Configurations

Enterprise Backbone

Internet
Sometimes There Is A Separate DMZ For Close Partners

- **Internal Servers**
- **Internet-Facing DMZ**
- **User Workstations**
- **Partner Facing, or EXTRANET DMZ**
- **Internet**
  - To Partners
The Extranet DMZs May Be Attached to a Private Network, or *Extranet*
Unclassified Sharing in the Interagency?

One Result of the Trusted Internet Connection Initiative?
Other TIC Thoughts Based on DoD Lessons

• DoD has evolved various connection approval, compliance assessment, enforcement, and exception processes
  – These will likely need to be replicated in the inter-agency
  – Compliance enforcement must have teeth

• Partners ALWAYS have internet connections so connect to them via partner/extranet DMZs and monitor these as you would an internet connection

• Clear lines of authority for management of the connections is essential

• Sharing the attack detection and diagnosis data from the connection points is essential
A Little Bit About Driving Out Anonymity:

**PKI and Cyber Identity Credentials**
*(DoD PKI and Other PKIs)*
First, a bit about Bad Guys and Directories
(and why we have Public Key Infrastructures)
Publishing Public Keys: the old days

...One public key looks pretty much like any other

The Directory

<table>
<thead>
<tr>
<th>Bill Smith</th>
<th>A Public Key</th>
</tr>
</thead>
<tbody>
<tr>
<td>John Smith</td>
<td>A Public Key</td>
</tr>
<tr>
<td>Sam Smith</td>
<td>A Public Key</td>
</tr>
</tbody>
</table>
Publishing Public Keys: Now

<table>
<thead>
<tr>
<th>Bill Smith</th>
<th>A Public Key</th>
<th>Trustworthy Third Party’s Signature That Binds the Name and Key Cryptographically</th>
</tr>
</thead>
</table>

Increased *assurance* that Bill’s public key is really his, and not John’s or Sam’s
An Important Detail…

• Bill still needs to protect the other piece of the credential…the *private key*
The DoD PKI

- Primarily identity credentials for people (for now)
- Issuance tied to the pool of people identity in DoD...DEERS
- Single trust root, although credentials issued by many subordinate certificate authorities
- **Asserts very little other than the tie between a name and a public key**
  - Must find those other tidbits about Richard Hale from other sources
- Private keys (mostly) stored on the Common Access Card, or CAC
- Credential quality depends on many, many things...
DoD PKI Credential Quality
(How Much Can I Trust This Credential I’ve Been Presented?)

- Use of DEERS Identity system
- Use of Hardware Crypto in CAs
- Use of hardware token (CAC) for the private key
Lots of Assurance Increases in the Works for DoD & Other PKIs

• Improved cryptography (elliptic curve)
• Stronger protection of private keys, alternate tokens
• Better identity vetting of individuals before issuing a credential
• Stronger protocols between the certificate authority and the place the keys are generated
• More auditing
• Etc., etc., etc.
Sharing & Application Agility: The Service Oriented Architecture

(We’ll come back to my cyber identity credential, and some of its uses)
The Simple View of the SOA

Service Interface

Service Provider

Service Consumer

The WAN
What’s Behind the Service Interface?

The WAN

Hosting Center
Dependable SOA Poses a Question

- Each service consumer relies on some sort of statement by the service provider on the service being consumed
- Provider asserts things like
  - Reliability of the service (in the face of equipment failure, circuit failure, natural disaster, cyber attack, whatever)
  - Accuracy of information
  - Performance, etc.

How does the consumer know whether to believe the claims?
Answers?

• Traditionally, a contract between supplier and consumer defines the terms of service
• In DoD and the IC, this isn’t exactly how we work
• But, we could invent a scheme of point-to-point MOAs. But, this doesn’t scale, even if we could figure out enforcement
• But, important missions, people’s lives, and all sorts of things may depend on the service

So, I think a third party must verify the service providers’ claim, then publish the findings
  – (a Certifier, a Tester?)
Who Spot Checks These Claims?

• To ensure the service provider is continuing to satisfy the claims on which our consumer is depending
• Certifier?
• Tester?
• Blue Team? (Acting on behalf of both the consumer and the provider?)
Isn’t This a Lot of Trouble Over Something That’s Not That Hard?
Composition of Services into an Application

Our service is a participant in a composed application serving a soldier in the field
Many Service Providers

“Dependability in the Face of Cyber Attack”
Back to Sharing While Keeping a Secret
If We Have Thousands of Services, Can an Access-Control-List Access Model Work?

Enter … **Attribute-Based Access Control**

• Important in the SOA going forward
  – Scale
  – Policy flexibility *(share information with unanticipated person without having to give the person an account)*
Before:
Allowing me to access information,
Allowing me to act in a certain role,
Doing business with me, etc.

Step 1. **Determine that it’s really me**

Step 2. **Then, learn things about the real me**
before deciding to take a risk on me
Step 1: I present my PKI credential and use my private key to authenticate.

Then, all that stuff about me comes into play
Who Knows, Who Tells the Things About Me?

I Do

But if you don’t know me, will you trust what I say?

Others Do

You might trust some of what others say about me (attributes about me)
Attribute-Based Access Control

Service Consumer

Request (with PKI authentication)

Policy Enforcement Point

Policy Decision Service

Data

Service Provider

Attributes

Attribute Store

Attribute Store

Man or Machine
Are Those Attributes Worthy of The Service Provider’s Trust?
Attributes and the Directory Problem

- Tight tie between me and my public key provided by my PKI cert (and by careful design of the issuance process)
- Where’s the tight tie between me (my name or some other unique identifier) and an attribute about me?
- Who is authoritative for particular information about me?

How does a relying party know that my credit score, my clearance, my role, my grades, are really mine?
Incident & Attack Detection, Diagnosis, and Reaction
The Computer Network Defense Process

- **Detect** the incident or attack or problem (hopefully before it’s launched)
- **Diagnose** what’s going on
- **Develop** militarily useful courses of action
- **Pick** one
- **Execute** it
- **Then follow up**

*All in militarily useful time*
Realistic NETOPS Tactics, Techniques, Strategies

- This may (at any time) be a war fight
- Development of effective NETOPS war fighting tactics, etc. must be done by considering realistic adversaries
- Then we must practice these (and practice, practice, practice these)
- Practice at all levels of organizations, from individuals to small groups to ops centers to multiple ops centers…
  - You get the idea
This Also Requires Broad Sharing

- Sharing of raw sensor data, partial incident data, and more fully analyzed incidents is also critical
  - If we’re to do this fast, and broadly across government and industry
  - So, IMHO we’ve got to set standards for protecting this stuff so we’re all willing to share...
DoD Sets Standards and Accredits Computer Network Defense Service Providers

• The Interagency, industry, others will likely have to do this too
To Summarize...
1. Dependability in the Face of Cyber Attack

2. Keeping a Secret

Both While Simultaneously Sharing Information Broadly
DEFENSE INDUSTRIAL BASE
SECTOR COORDINATING COUNCIL

Improving the Sharing and Reliability of Public and Private Threat and Hazard Information

April 9, 2008
Panel Objectives/Takeaways

- Objectives
  - Exchange information
  - Discuss gaps and opportunities for better provision/utilization of global threat and natural disaster intelligence
  - Explore case studies, best practices, and successful strategies for combating and understanding the insider threat
  - Identify opportunities for public/private intelligence sharing partnerships

- Takeaways
  - Information sharing, integration mechanisms, and how they enhance rapid response
NIPP Implementation Actions

“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 CI/KR 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.
Improving Information Sharing

• Numerous models of mechanisms that work …
  – Google “Info Sharing” 20,400,000 hits
  – Google “Trust Models” 2,730,000 hits

• Implies “no ideal”
  – Contemporaneous venues with similar objectives are okay
  – Helps bridge blockers
  – Cues parties to desired common solution
  – Enriches information streams
  – Builds relationship opportunities
    • Dialogue between DIB and DoD

• Gaps
  – Includes policy, classification, communication system issues
  – Issues enhance or impede key “lubricants”
    • Trust, confidence, shared equity
Business Structure

- DIB companies have grown to large entities through the acquisition process
- Many unknowns come into play
  - Policy differences
  - Cultures
  - Vetting procedures
  - Foreign connections
  - Organizational control
CI Strategy for Business

- Companies must realize they have a real threat present
- Senior Management must support the CI effort or it will not work
- Awareness of the workforce is key to success
- Have a CI program in place with trained personnel to manage it
Government Interface with the DIB

• Not all companies are managed the same in regards to security
  – Legal Department
  – Human Resources Department
  – Operational Management

• Be aware all have their own equities to protect
Government Interface

- Important to establish key relationships early
- Ensure “hand-offs” are handled appropriately
- Attempt to limit the amount of agents dealing with a particular firm, i.e., cyber, humint, etc.
- If possible, manage interface through the senior security official
- Offer various support assistance to firm
Issues remaining

- Lack of collection capabilities
- Lack of efficient means of secure data access and dissemination
- Training, investigative resources
- Duplications of efforts (multi-agency overlap)
Cyber Issue

- #1 issue facing industry
- Lack of convergence between security and IT functions exist in some companies
- Being treated as an “Information Assurance” issue, not as an “Intelligence” issue
- No real solutions being developed to halt threat as long as firms continue to operate and store data connected to the internet
SUPPLY CHAIN PREPAREDNESS AND RESPONSE MANAGEMENT

Defense Industrial Base – Critical Infrastructure Protection Conference
8 April 2008

John F. Rank
Vice President, Supply Chain Management
General Dynamics Land Systems, and
Chair, General Dynamics Supply Chain Management Council
A CAUSE FOR ACTION…

- U.S. Government Mantra & Policy
- An Industrial Base Perspective
- What Can and Should Supply Chain Management be Doing?
DIB CIP CONFERENCE
A CAUSE FOR ACTION


  Policy

  - Enhance protection of critical infrastructure and all key resources to assure no negative affect or cascading disruption
  - Protect transportation systems
  - Secure IT systems (Cyberspace)
  - Department of Defense (DoD) designated to cover Defense Industrial Base Infrastructure
Coordination with Private Sector

- Collaborate and Support Private Sector Coordinating Mechanisms
- Prioritize the Protection of Critical Infrastructure and Key Resources
- Facilitate Information Sharing

U.S. Government Agencies and Industrial Base are Partnering on Preparedness and Response
  ➤ “This directive establishes policies to strengthen the preparedness of the United States to prevent and respond to threatened or actual domestic terrorist attacks, major disasters, and other emergencies…”
Defense Industrial Base (DIB)
Sector–Specific Plan (SSP)

- Guidance Developed by **Collaboration of Industry and U.S. Government** Security Partners

- Plan covers:
  - Goals
  - Identification of Assets
  - Assessment of Risk and Risk Management
  - Asset Prioritization Model (APM) which includes (16) factors classified into: (5) Mission, (5) Threat, (4) Economic, and (2) “Other”
  - Development of Protective Systems
  - Measurements on Progress/Goals
  - Research and Development
  - Management and coordination of the Sector Specific Agency (SSA)
We Cannot be Complacent

- Al-Qaeda has a 20 Year Plan
  - Total Confrontation by 2016
  - Definitive Victory by 2020
    - Will focus on “Critical” Infrastructure
- Goal Should be to Make the U.S. Industrial Base Strive to Make Nothing Critical
- A “Sense of Urgency When There is no Emergency”
An Industrial Base Perspective

General Dynamics and it’s Supply Chain Challenges
General Dynamics Corporation

Corporate Overview

Business Segments

Combat Systems

Land Systems
General Dynamics Corporation

Charlie Hall
Executive VP
Combat Systems

Nick Chabraja
Chairman & CEO

Jerry DeMuro
Executive VP
IS & T

Mike Toner
Executive VP
Marine

Joe Lombardo
Executive VP
Aerospace

DIB CIP CONFERENCE

Revenues: $27 Billion
Employees: 82,500

Combat Systems

Information Systems & Technology

Marine

Gulfstream

General Dynamics Corporation

• Revenues: $27 Billion
• Employees: 82,500

Charlie Hall
Executive VP
Combat Systems

Jerry DeMuro
Executive VP
IS & T

Mike Toner
Executive VP
Marine

Joe Lombardo
Executive VP
Aerospace

Approved for Public Release, Distribution Unlimited, GDLS
approved, fsc 2008-13, dated 4/4/08

SCM
Supply Chain Management
14 April 2008
GD Land Systems (GDLS)  
Full Spectrum Product Offering

- **Warrior**  
- **Robotics**  
- **JLTV**  
- **LAV / Stryker**  
- **MRAP**  
- **Cougar**  
- **R-31**  
- **EFV**  
- **Abrams MBT**  
- **FCS**

Approved for Public Release, Distribution Unlimited, GDLS approved, log 2008-13, dated 4/4/08

**GENERAL DYNAMICS**  
Land Systems

**SCM**  
Supply Chain Management  
14 April 2008
CY2007 Overview

- Combat Vehicles and Subsystems
- Global Business Base
- 9,100 Employees
- ISO “9001-2000” Registered
- SEI Level V Certified

Multiple Products & Multiple Customers

- Stryker 8x8: 33%
- Abrams Tanks: 27%
- Light Armored Vehicle: 12%
- Mine Protected Vehicles: 9%
- Future Combat Systems: 9%
- Robotics: 3%
- Expeditionary Fighting Vehicle: 3%
Multiple Locations

- Ft. Wainwright
- Ft. Richardson
- Ft. Lewis
- Schofield Barracks
- Pohakuloa Training Area
- Camp Pendleton
- Ft. Hood
- GDLS Central Office – GDLS Logistics & Engineering Center
- Joint Systems Manufacturing Center
- Anniston Army Depot
- Muskegon Technical Center
- GDLS Future Combat Systems
- Shelby Operations
- Scranton Operations
- Robotic Systems
- Amphibious Systems
- Woodbridge Tech
- Tallahassee Operations

U.S. Locations

Approved for Public Release, Distribution Unlimited, GDLS approved, log 2008-13, dated 4/4/08
DIB CIP CONFERENCE

International Locations

GDLS - Canada
London, Ontario

Edmonton, Alberta

GDLS - Australia
Adelaide, Australia
Land Systems - Supply Chain Exposure

- > 60% of Sales Revenue is Through Purchased Products & Services
- Over 3600 Suppliers
- 180 Critical Suppliers
- 250 Offshore Suppliers
- 2007 Spend was $2.2B
Industrial Base

- Critical Subsystems & Commodities
  - Mills for Raw Material
  - Heavy Fabrications
  - Mission Equipment; Fire Control, Electro-Optical
  - CLS Support Structure; Repair and Overhaul, Spares
  - Survivability and Armament
  - Subsystem Assemblies

U.S. defense products contain many subsystems which are custom designed and unique
## GDLS Partnerships on Major U.S. Platforms

<table>
<thead>
<tr>
<th>PROGRAM</th>
<th>MULTIPLE INDUSTRY PARTNERS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Future Combat Systems (FCS)</td>
<td>BAE</td>
</tr>
<tr>
<td>Abrams and Bradley Modernization</td>
<td>BAE</td>
</tr>
<tr>
<td>Mine Resistant Ambush Protected (MRAP)</td>
<td>Force Protection (Force Dynamics)</td>
</tr>
<tr>
<td>Joint Light Tactical Vehicle (JLTV)</td>
<td>AM General (General Tactical Vehicles)</td>
</tr>
</tbody>
</table>

**Shared Procurement Responsibilities**
THREATS TO THE DEFENSE SUPPLY CHAIN INFRASTRUCTURE

A BROAD PERSPECTIVE

WHAT CAN AND SHOULD WE BE DOING?
DIB CIB CONFERENCE

Theme for Supply Chain Management Portion of the Conference:

“Threats to the supply chain, programs and action to mitigate security and continuity challenges, and approaches to foster supply chain response.”
SUPPLY CHAIN INFRASTRUCTURE

Affect on Business if Disruption or Security Breach

- Loss of Customer Confidence
  - Company Image

- More U.S. Government Oversight

- Loss of Revenue

- Legal Issues
What are the threats:

- **Terrorists / Activists**
  - Acts
  - Ownership of Suppliers

- **Acts of War**

- **Disasters**
  - Tornados, hurricanes, floods, wild fires, earthquakes
  - Industrial Fires
  - Blackouts
  - Environmental
SUPPLY CHAIN INFRASTRUCTURE

- IT/Cyberspace/Telecommunications
  - Disruptions
  - Infiltration
- Work Stoppages
  - Sabotage
- Financial Stability
- Customs (Foreign & Domestic) and Border Issues
- Political Instability
- Civil Disturbance
SUPPLY CHAIN INFRASTRUCTURE

Global Procurement Adds Another Dimension to Control and Protection

- Import Control
- U.S. Government Agency Infrastructure and Support is Limited
- Legal Action and Enforcement of Contracts and Purchase Orders
- Political and Civil Unrest
What Can and Should Supply Chain Management (SCM) be Doing?
What Should SCM Do?

Recognize the Broad Spectrum of the Supply Chain that can be Affected

- Procurement
  - Suppliers
    - Domestic & Offshore
  - Manufacturing Locations
- Distribution & Transportation
  - CONUS & Imports
- Customers
- End Users/War Fighter
What Should SCM Do?

- Recognize that the Supply Chain is Interconnected:
  - There are Multiple Exchanges Along the Continuum
  - If one piece of the Supply Chain Link is Harmed or Fails, There can be a Major Impact
  - Trying to Protect the Entire Supply Chain may be Impractical or Impossible
    - However, the Threats and Need for Protection cannot be Ignored
What Should SCM Do?

- Recognize There is a Cost
  - The Cost of Supply Chain Security is Anticipated to Exceed $151B, Annually *
  - Cost of Prevention Versus the Risk of Loss is a Difficult Balance
    - Is There A Return On Invested Capital (ROIC)?

* “Five Tenants of Security – Aware Logistics and Supply Chain Operations”, by Dawn M. Russell and John Saladana in Transportation Journal
What Can We do to Protect the Supply Chain and Make it More Resilient?
What Should SCM Do?

Protection and Resiliency

- Catastrophic Risk Management should be an Element of Business Strategy

- Flexibility and Redundancy must be Added to the Supply Chain in Order to be Proactive When Disaster Strikes
  - Cost Issue

- Security and Planning are Key
What Should SCM Do?

- Preparedness Should be a Way of Thinking
  - Requires Adoption of a Security-Minded Culture

- Program Training, Awareness, and Maintenance are Essential for Execution
  - Must Flow Down

- A FORMAL PLAN is Needed
  - How to Protect Resources
  - How to Recover Quickly

- A Common Guideline or International Standard Needed?
What Should SCM Do?

Anticipate and Assess Risk Levels:

- With Suppliers
  - Alternate Sources
- Transportation Modes
- Warehousing
- Availability of Alternate Work Sites
- Threat to Intellectual Property
- Allocation of Resources
  - Can They Work Remotely?
What Should SCM Do?

- **IT Solutions**
  - Data Back Up
  - Manual Approach
    - Electronic Purchase Orders
  - Equipment Availability
    - Blackberry Back Up
- **Telecommunications**
  - Land Lines and Cell Phones
- **Interdependency Analysis**
- **Benchmark Industry**
What Should SCM Do?

Develop an **Executable** Disaster Business Continuity and Recovery Plan

- Focus on Safeguarding: People, Assets, Financial Stability, Customer Deliverables
- Determine How to Assure Business Continuity
- Identify threat Deterrents
- Development of Plan Requires Collaboration with:
  - Industrial Security
  - IT Support
  - Human Resources
  - Operations/Manufacturing
  - Government Agencies
  - Industrial Supply Base
What Should SCM Do?

Crisis Communication and Contact Plan

- Need Points of Contact (POC) that are Readily Available
  - Suppliers
  - Internal
    - Industrial Security
    - Human Resources
    - Operations/Manufacturing
    - Leadership
  - Customers
  - U.S. Government Agencies
  - Employees
    - Key Employees
    - Cascading Contact Plan
What Should SCM Do?

- Contact Plan Requires POC Information:
  - Name & Title/Role/Responsibility
  - Land Line Telephone Number
  - Cell Phone Number
  - Home, if Possible
  - Alternate POC
What Should SCM Do?

- **Determine How Long of a Downtime Period the Business can Sustain**
  - Number of Days/Weeks by Internal Function and/or Supplier

- **Determine Recovery Time Lines**
  - Facility Availability
  - Resources
  - IT and e-Business Systems Operation
    - MRP
    - Electronic Purchase Orders
    - Documentation and Release Data
    - Logistics and Routing
    - Finance
Supply Chain Vulnerability is Underestimated. So, What can We do with the Industrial Supply Base Beyond Exchanging POC Information?

- Assess Where Weak Links may be
- Require Security and Preparedness Plans from Critical Suppliers
- Encourage Customs-Trade Partnership Against Terrorism (C-TAPT) Certification or Similar Involvement
- Review Who is Involved in Their Manufacturing and Distribution Chain
  - Lower Tiers, also
What Should SCM Do?

- Develop Alternate Suppliers for Critical Items
  - Offshore Suppliers Backed up by Domestic Sources or from Alternate Low Cost Countries
    - Utilize 3rd Party Advisory Consultants to Validate Suppliers

- Have Alternate Freight Carriers and Modes of Transportation Available

- Apply Technology
  - Radio Frequency Identification (RFID)
  - Smart Chips
What Should SCM Do?

Summary:

- Recognize there is Cause for Action
- Collaboration Between Industry, it’s Supply Base, and U.S. Government Agencies is Mandatory
- Assess Threats and Vulnerability
- Create the Plan, Policies, and Procedures
- Assess the Level of Maturity of the Plan and Execute Accordingly
  - Implementation is Top Down
- Monitor and Measure
Questions
THE BUSINESS OF CYBER VULNERABILITIES

Aaron Turner – CISSP, CISM
Idaho National Laboratory & I³ Partners
A historical view of the volume of security problems that have impacted computing systems in the last 7 years.

Severity Increasing
Increasing attacker efficiency is shown in the number and percentage of high-severity vulnerabilities that can be used for targeted attacks.

Vulnerability Trends
‘Ubiquitous Applications’ like Acrobat and Flash are providing new exploitation opportunities.

OS vs non-OS Vulnerabilities
Potential new category: “Search Vuln.”

Industry-wide Problem
Skilled attackers are equal-opportunity exploiters. A listing of high-severity vulnerabilities from 2007 shows just how pervasive the problem is.

<table>
<thead>
<tr>
<th>Vendor</th>
<th>Vulnerabilities</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Microsoft</td>
<td>148</td>
<td>4.3%</td>
</tr>
<tr>
<td>Novell</td>
<td>132</td>
<td>3.8%</td>
</tr>
<tr>
<td>Red Hat</td>
<td>127</td>
<td>3.7%</td>
</tr>
<tr>
<td>Ubuntu</td>
<td>115</td>
<td>3.3%</td>
</tr>
<tr>
<td>Apple</td>
<td>110</td>
<td><strong>3.2%</strong></td>
</tr>
<tr>
<td>Sun</td>
<td>85</td>
<td>2.5%</td>
</tr>
<tr>
<td>PHP</td>
<td>72</td>
<td>2.1%</td>
</tr>
<tr>
<td>Oracle</td>
<td>68</td>
<td>2.0%</td>
</tr>
<tr>
<td>Cisco</td>
<td>62</td>
<td>1.8%</td>
</tr>
<tr>
<td>Mozilla</td>
<td>48</td>
<td>1.4%</td>
</tr>
</tbody>
</table>

*Full Point Increase vs ‘06*
A historical view of the volume of security problems that have impacted computing systems in the last 7 years.

Where is the missing 35%?
‘Ubiquitous Applications’ like Acrobat and Flash are providing new exploitation opportunities.

Vulnerability Trends

Potential new “Search” class of vuln.
Increasing attacker efficiency is shown in the number and percentage of high-severity vulnerabilities that can be used for targeted attacks.
Skilled attackers are equal-opportunity exploiters. A listing of high-severity vulnerabilities from 2007 shows just how pervasive the problem is.

<table>
<thead>
<tr>
<th>Vendor</th>
<th>Critical Vuln’s</th>
<th>%</th>
</tr>
</thead>
<tbody>
<tr>
<td>Microsoft</td>
<td>148</td>
<td>4.3%</td>
</tr>
<tr>
<td>Novell</td>
<td>132</td>
<td>3.8%</td>
</tr>
<tr>
<td>Red Hat</td>
<td>127</td>
<td>3.7%</td>
</tr>
<tr>
<td>Ubuntu</td>
<td>115</td>
<td>3.3%</td>
</tr>
<tr>
<td>Apple</td>
<td>110</td>
<td><strong>3.2%</strong></td>
</tr>
<tr>
<td>Sun</td>
<td>85</td>
<td>2.5%</td>
</tr>
<tr>
<td>PHP</td>
<td>72</td>
<td>2.1%</td>
</tr>
<tr>
<td>Oracle</td>
<td>68</td>
<td>2.0%</td>
</tr>
<tr>
<td>Cisco</td>
<td>62</td>
<td>1.8%</td>
</tr>
<tr>
<td>Mozilla</td>
<td>48</td>
<td>1.4%</td>
</tr>
</tbody>
</table>

Full percentage point increase since ‘06
The Economics of Vulnerabilities

- An underground economy has been established for the production, distribution, exchange and purchase of vulnerabilities
- As with any economic system, the attacker community has succeeded in discovering efficiencies through specialization of labor
  - Vulnerability Factories
  - Vulnerability Wholesalers
  - Vulnerability Transporters
  - Vulnerability Consumers
- Examples:
  - 76service.com
  - Executive Phishing Services

The Vulnerability Market

In 2006, a complex vulnerability was discovered through telemetry from Microsoft’s sensor networks.

Through further investigation, it was determined that the level of effort required to research the vulnerability and develop the exploit would have required significant effort and manpower. Within weeks of the targeted attack, the exploit was seen for sale within underground economy channels.

Leading Vulnerability Economies: % of Vulnerabilities to # of Total Estimated Computer Users by Country

<table>
<thead>
<tr>
<th>Asia-Pacific</th>
<th>Middle East - Africa</th>
<th>Europe</th>
<th>The Americas</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mongolia   25.0%</td>
<td>Bahrain  8.7%</td>
<td>Albania  8.7%</td>
<td>Dom. Republic 9.4%</td>
</tr>
<tr>
<td>Thailand   8.2%</td>
<td>Egypt     7.0%</td>
<td>Turkey     7.1%</td>
<td>Brazil        7.4%</td>
</tr>
<tr>
<td>Macau SAR  8.1%</td>
<td>Iraq      6.9%</td>
<td>Romania    4.6%</td>
<td>Honduras      6.9%</td>
</tr>
<tr>
<td>Vietnam    7.5%</td>
<td>Morocco   6.7%</td>
<td>Portugal   4.4%</td>
<td>Jamaica      6.2%</td>
</tr>
<tr>
<td>Indonesia  6.8%</td>
<td>Saudi Arabia 6.7%</td>
<td>Russia     4.4%</td>
<td>Chile        6.1%</td>
</tr>
</tbody>
</table>
Special Thanks to:

Jeff R. Jones, Senior Security Strategist, Microsoft Corporation

All Vulnerability Data Referenced from:

Microsoft Security Intelligence Report
http://www.microsoft.com/sir

Additional Resources

Search Vulnerability:
- http://www.cio.com/article/135500/2
- Executive Phishing Services

Contact Information

aaron@i3partners.org
Agenda

- The Challenges We Face
- The National Security Environment
- DoD Preparedness & Response
  - Physical
  - Cyber
- Conference Challenge
Welcome

The DIB is a worldwide industrial complex with capabilities to develop and maintain military weapons systems to meet military requirements

- +250,000 Defense Industrial Base (DIB) Sites worldwide
- DIB is critical to our nation and the war fighter
- DIB assets support DoD missions
- Vital to the DoD execution of the National Military Strategy
- Our collective efforts make a difference in war fighter’s lives and missions

DoD values your contributions to maintain technologically superior, resilient industrial capabilities to preserve our nation’s security.
Nation-state threats will continue

- “Traditional” ballistic and cruise missile threats
- Rogue states employing asymmetric means
  - Both cyber and physical
- Potential emergence of a regional peer competitor

Natural Hazards

- Earthquake
- Flood, Tsunami
- Wildfire
- Health and Disease

Transnational threats will be the most pressing

- Terrorists will seek to:
  - Attack Americans and Western Allies at home and abroad
  - Inflict mass casualties or cause mass panic through CBRN means (e.g., CBRN weapons or conversion of civilian infrastructure or transport into WMD)
Challenges

- Collaboration
  - Partnership, shared responsibility, and Trust engendered by partnership
  - Information sharing and protection
  - Threat and warning information sharing

- HUMINT (Insider threat)

- Physical Threats and Hazards

- Cyber Security

“Each of us has an extremely important role to play in protecting the infrastructures and assets that are the basis for our daily lives and that represent important components of our national power and prestige. The success of our protective efforts requires close cooperation between government and the private sector at all levels.”

- President George W. Bush
Mission Assurance Concept

- Improve DoD’s ability to execute its Mission Essential Functions in a stressed environment through integrating key programs & activities

- Comprehensively evaluate risk to DoD missions, including the unintended consequences of base consolidation & realignment

- Enable Senior Leader’s ability to refine mission-related policies, plans, programs, resources, and activities, and more productively link policy decisions to operational requirements through:
  - Organizational Effectiveness
  - Funding Efficiencies – Making better informed resource allocation (e.g. budgetary) decisions that increase oversight and accountability
  - Compliance – Coordinating and consolidating Measures of Effectiveness (MOEs)

*Mission Assurance is an integrating concept, NOT a change of ownership!*
Mission Assurance – A Value Proposition

Organizational Effectiveness
- Improves relations among segregated elements of an organization
- Integrates disparate elements
- Improves operational efficiency and mission effectiveness

Funding Efficiencies
- Improves cost control
- Improves access to funds through prioritized justification of needs
- Prioritizes funding and resource allocation

Compliance
- Assures commitment throughout organization
- Enhances readiness
- Establishes governance process internal to the organization
- Accounts for applicable legislative requirements

MISSION ASSURANCE

Organizational Effectiveness
(Policy & Planning)

Funding Efficiencies
(Resources)
Articulates DoD’s risk management approach required for ensuring the availability of assets deemed essential to the successful completion of DoD missions in an all-threat, all-hazard environment.

Defines through stated goals & objectives how DoD will protect Defense Critical Infrastructure (DCI) to achieve mission assurance:

- **Goal 1**: Provide DCIP policy and program guidance
- **Goal 2**: Foster DCIP strategic partnerships and enabling technologies
- **Goal 3**: Integrate and implement DCIP plans, programs, and capabilities at all levels
- **Goal 4**: Facilitate DCIP resourcing at all levels
- **Goal 5**: Promote DCIP education and outreach
DCIP Strategic Policy Timeline

2005
- 19 Aug
  - DODD 3020.40

2006
- 9 Jun
  - DCIP Benchmarks & Standards
- JUN
  - NIPP
- 13 Jul
  - Interim Implementation Guidance (IIG)
- 15 Sep
  - DIB Sector Specific Plan
- 20 Sep
  - Geospatial Data Strategy

2007
- 12 May
  - DCIP Security Classification Guide (SCG)
- MAY
  - DIB SSP
- 15 May
  - Infrastructure Resiliency Guide (IRG)
- JUN
  - DIB Sector Annual Report
- 7 Jun
  - DCIP Standards & Benchmarks (Update)

2008
- 12 Mar
  - BEI for DCIP TCAs
- 18 Mar
  - DODI 3020.nn
- 7 Jun
  - Strategy for DCI
- 7 Jun
  - CAIP Manual
- 7 Jun
  - Remediation Planning Manual
- 7 Jun
  - DCA Risk Decision Manual
- 7 Jun
  - Security Classification Manual
Partnering Leads to Real Success

- Rotating electrical equipment / control system vulnerability
- CIP-MAA assessment visits – information for owner/operator use
- BZPP provided resources to improve first responder capabilities
- Providing security awareness training for DIB partners

Government and Private Sector

- Team effort to produce the Sector Specific Plan – continues to grow
  - CIPAC public / private working group on Goals and Objectives
  - CIPAC public / private working group on cyber security
- DCMA and DHS Protection Security Advisor visits

Canadian Dept of National Defence (DND)

- Establishing mutual awareness and assessment program (e.g. Joint Strike Fighter)
Partnering Efforts

- **DoD-DIB Information sharing**
  - Providing best practices, expertise and information

- **DoD-DIB collaboration on response actions**
  - Response actions
  - Self-assessments

- **Protected Critical Infrastructure Information (PCII)**
  - Protects voluntarily submitted critical infrastructure information (CII) from public release under FOIA, civil litigation, and state and local “sunshine” laws.
  - ASD (HD&ASA) continues to pursue DoD accreditation under this program.

*Leverage trust for two-way communication and share information for a shared purpose – assured availability*
Hostile nations still pose a cyber threat to the United States because they have the intent and technological capabilities to do so.

A cyber attack could substantially impact a number of sectors in the United States, including agriculture, emergency response and preparedness systems, transportation, energy, health care, financial services, and telecommunications.
Cyber Security

- Cyber Security is a **National Effort**
  - DHS is lead agency for domestic cyber security
  - DoD will fully support national efforts with policy coordination, information sharing, and technology transfer

- DepSecDef directed USD(P) to lead **Cyber Security Task Force**
  - Chartered to implement NSPD-54/HSPD-23, Cyber security Policy
  - DoD members include NII, SOLIC, ATL, J5, Air Staff, and JTF-GNO
  - Interagency partners include DHS, DOJ, OTSP, DNI, and NSA

- ASD HD&ASA has DoD DCIP **mission oversight and policy responsibility**
  - Lead cyber security coordinator for DoD
  - Best positioned to interface with the interagency and leverage existing capabilities and competencies within DoD

*Provide unity of effort across the Department and coordinate with interagency partners to improve national security against the full spectrum of cyber threats*
Conference Challenge

- What do you perceive as the greatest threats to CI/KR IT and communications networks?

- What are gaps and barriers to effective bi-directional information sharing?

- What types of information sharing are existing public-private partnerships and structures best at addressing?

- How can we share best practices, products, and standards?

- What existing and emerging technologies do you believe are most essential to enhanced CI/KR network security?
2008 DIB Critical Infrastructure Protection Conference & Technology Exhibition

QUESTIONS?
WE'RE AT WAR

ARE YOU DOING ALL YOU CAN?