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?
Homeland Security Presidential Directive 7

- 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)

- 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)
A CAUSE FOR ACTION

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

Jerry DeMuro
Executive VP
IS & T

Mike Toner
Executive VP
Marine

Joe Lombardo
Executive VP
Aerospace

Nick Chabraja
Chairman & CEO

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

Revenues: $27 Billion
Employees: 82,500

Combat Systems
Information Systems & Technology
Marine
Gulfstream

General Dynamics Corporation

Marine

Charlie Hall
Executive VP
Combat Systems

Jerry DeMuro
Executive VP
IS & T

Mike Toner
Executive VP
Marine

Joe Lombardo
Executive VP
Aerospace

Nick Chabraja
Chairman & CEO

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

Revenues: $27 Billion
Employees: 82,500

Combat Systems
Information Systems & Technology
Marine
Gulfstream

General Dynamics Corporation

Marine

Charlie Hall
Executive VP
Combat Systems

Jerry DeMuro
Executive VP
IS & T

Mike Toner
Executive VP
Marine

Joe Lombardo
Executive VP
Aerospace

Nick Chabraja
Chairman & CEO

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

Revenues: $27 Billion
Employees: 82,500

Combat Systems
Information Systems & Technology
Marine
Gulfstream

General Dynamics Corporation

Marine

Charlie Hall
Executive VP
Combat Systems

Jerry DeMuro
Executive VP
IS & T

Mike Toner
Executive VP
Marine

Joe Lombardo
Executive VP
Aerospace

Nick Chabraja
Chairman & CEO

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

Revenues: $27 Billion
Employees: 82,500

Combat Systems
Information Systems & Technology
Marine
Gulfstream

General Dynamics Corporation

Marine
GD Land Systems (GDLS)
Full Spectrum Product Offering

Warrior

Robotics

JLTV

LAV / Stryker

MRAP

Cougar

R-31

EFV

Abrams MBT

FCS

GDSL LEad

MCS

RSV

CZV

Common Chassis

GENERAL DYNAMICS
Land Systems

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

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

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

- GDLS - Canada
  - Edmonton, Alberta
  - London, Ontario
- 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
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?
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
SUPPLY CHAIN INFRASTRUCTURE

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 Should SCM Do?

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
What Should SCM Do?

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