A research agenda for supply chain security and productivity

Chelsea C. White, III
Alan L. Erera
Martin W.P. Savelsbergh

School of Industrial and Systems Engineering
Georgia Institute of Technology

August 31, 2004
1 Introduction

Supply chain security has emerged as an area of vital importance for both the users and providers of the freight transportation system. This importance is in large part due to the economic importance of international trade to the United States; trade currently generates 23% of U.S. Gross Domestic Product. Possible future terrorist attacks on the U.S. may make use of the international and/or domestic freight transportation system, and such attacks may have devastating consequences in terms of fatalities and economic destruction [O’Hanlon et al., 2002]. As an example, the economic impact on U.S. supply chains due to higher shipping costs, increased travel times, increased inventories, border delays, and other changes as a direct result of the 11 September 2001 terrorist attacks is estimated to be $150 billion per year [Bernasek, 2002].

The security of any system needs to be defined relative to a threat or set of threats. In the past, many supply chain operators’ interest in freight security primarily focused on protecting against theft. Theft of goods-in-transit clearly affects firm profits. Supply chains therefore are led by market mechanisms to prevent theft; shippers want to avoid theft-related costs, and providers want to prevent theft to attract shippers concerned about theft-related costs. A firm may decide to adjust its inventory reordering strategies, modify the routing of freight, or change transportation service providers, if it believes that such decisions increase protection against theft. This demonstrates that enhanced security may lead to increased costs and potential loss of productivity.

Recent events have created a fundamental shift in thinking regarding the types of threats that may affect supply chain systems. Supply chain and freight transportation security now typically refers to a state of protection against various terrorism threats, most notably the weaponizing of the freight transport vehicle (e.g. container, ship, aircraft, train, truck). Smuggling of terrorists and terrorist weapons using freight containers is another major threat.

It should be clear that security against terrorist threats, similar to security against narcotics smuggling or security against hazardous materials spills, is a public good in the parlance of economics. Market forces alone may not provide incentive for firms to protect against supply chain terrorism threats. Since risk probabilities are perceived to be very small and potential consequences are difficult to measure, firms are unlikely to bear protection costs. However, the potential societal impact of terrorist attacks to supply chains and/or the transportation infrastructure supporting supply chains is high, and therefore societies have begun to employ regulation to ensure some degree of supply chain security.

One of the recommendations of the United States 9/11 commission is to broaden the focus of transportation systems security efforts [NCTA, 2004]. Importantly, the
report notes that currently more than 90% of U.S. transportation security funding is directed at the passenger aviation sector. The report correctly points out that security vulnerabilities exist within other transportation systems, notably cargo, and recommends that the “U.S. government should identify and evaluate the transportation assets that need to be protected, set risk-based priorities for defending them, select the most practical and cost-effective ways of doing so, and then develop a plan, budget, and funding to implement the effort.”

Much attention has been focused on the economic impact of security concerns and resulting regulatory initiatives on the users (e.g., supply chains) and providers (e.g., ports, trucking, shipping, and air cargo companies) of the freight transportation system. The design and operation of supply chain systems that provide both security against terrorist threats and also cost-efficient freight mobility is not always simple. Emerging security concerns affect all freight transportation modes (e.g., air, ocean, rail, highway, pipeline) and all components of the system:

- The physical infrastructure, e.g., roads, bridges, tunnels, seaports, airports, plants, distribution centers, warehouses, pipelines and pipeline pumping stations.
- The information infrastructure, e.g., traffic operations centers, communications systems for mobile assets.
- People, e.g., truck drivers.
- Cargo, e.g., containers, hazardous materials.
- Vehicles, e.g., ships, trains, trucks (power units, trailers, chasses), airplanes.

It is timely to ask: What are the resulting basic and applied research challenges for the industrial engineering and operations research community? What are the educational implications and issues?

The remainder of this report details a proposed research and education agenda for the industrial engineering and operations research community focused on important issues in supply chain security and productivity. Section 2 provides a small set of illustrative examples of security-related supply chain productivity challenges and opportunities. Section 3 describes the supply chain security workshop event held at Georgia Tech in February 2004. Section 4 describes in detail the proposed research and education agenda, highlighting a number of critical challenges and opportunities. Finally, Section 5 briefly explores the relationship between information technology and supply chain security.
2 Security challenges and opportunities

An illustrative example of a security-related disruption on supply chains is the increased length and variability of the time required for inspections of freight crossing U.S. international borders. Currently, the U.S. and Mexico support $250 billion per year in goods trade, while U.S. and Canada goods trade is valued at $475 billion. According to press reports, lines of southbound trucks full of Canadian auto parts, paper products, and other merchandise began to grow the evening of 18 March 2003 leading to queue waiting times of two hours–four times the normal average–at the Ambassador Bridge connecting Detroit and Windsor, Canada. How are the affected supply chains best designed and managed and what are the impacts on business practices such as just-in-time manufacturing? Tailored sourcing, with at least part of the supplier base within the national border of the assembler and the home market, may be a partial solution. What would be the long-term implications on international trade?

An example of a security-related regulatory initiative is the Container Security Initiative that places U.S. Customs agents at foreign seaports (currently, at the mega-ports, such as Rotterdam, Singapore, and Hong Kong) to inspect U.S.-bound containers offshore, prior to arrival at U.S. seaports. In 2002, over 7 million sea cargo containers arrived for import at U.S. seaports. Experts on terrorism, including those at the Federal Bureau of Investigation and at academic, think tank, and business organizations, have concluded that containers are vulnerable. A 2002 simulation of a terrorist attack in which radioactive bombs were discovered in cargo containers resulted in leaders shutting down every seaport in the United States for a number of days, resulting in a $58 billion revenue loss to the U.S. economy [Stana, 2004].

A number of important design and operations problems arise in the design and operation of maritime container supply chains with inspections. What is the most efficient port operations strategy for unloading and loading sea containers, given that a percentage of the containers require security inspections before being loaded onto outbound ships? What is the impact on seaport productivity, as a function of the percentage of containers to be inspected and how does this affect the efficiency of the supply chains using the port? What is the best time for the port to be provided by U.S. Customs with the list of containers to be inspected in order to maximize port productivity and the efficiency of the supply chains using the port?

An example of a potential opportunity provided by sophisticated security technology is the use of active smart seals to increase vendor-managed inventory practices. Vendor managed inventory is known to reduce inventory holding as well as transportation costs in many supply chain systems, but relies heavily on the technological capability to monitor inventories and consumption by consumers. Active smart seals provide the capability
to know the location and content of shipments anywhere at any time. This knowledge may enhance our ability to apply vendor managed inventory principles or even introduce them in industries where this was previously impossible. In general increased visibility leads to more effective supply chains.

3 The workshop

A one and one-half day workshop was held in Atlanta on 4 and 5 February 2004 that was supported by the National Science Foundation and the Trucking Industry Program and was hosted by Georgia Tech on the Georgia Tech campus. The workshop purpose was to identify key research and educational issues, problems, and opportunities associated with the security and efficiency of the freight transportation system. Perspectives from all of the various stakeholder groups were sought, where the stakeholders considered were the regulators, technology providers, users, and providers of the international freight transportation system. The assumption was that these key issues might have implications at several levels, e.g., operational, firm, and policy. The targeted research community was the operations research and industrial engineering community. The intent was to engage this highly resourceful, and talented community to address the security-related issues, problems, and opportunities that the nation is facing and will likely face in the future.

The approach taken was to have researchers:

- Listen to representatives from all of the stakeholder groups describe the issues, problems, and opportunities associated with transportation and supply chain security and productivity.

- Participate in breakout sessions to identify research challenges associated with the identified issues, problems, and opportunities.

- Convene a final panel to further refine these challenges.

The agenda for the workshop is presented in Appendix A. Workshop attendees, representing all of the aforementioned stakeholder groups, are listed in Appendix B.

4 A research agenda

Each of the breakout sessions at the workshop was asked to identify a list of important issues and compelling research challenges associated with the security and efficiency of the freight transportation system. In this section, we present a consolidated description
of the issues and challenges that were identified during these breakout sessions. We have synthesized the responses into a coherent research agenda.

We have organized the research agenda around two primary perspectives. The first perspective is that of a firm operating or participating in a supply chain or chains. The second perspective is that of society at large. We believe that it is imperative to make such a distinction for several reasons. In certain scenarios, market forces will compel supply chain firms to make decisions that lead to enhanced supply chain security. However, as we discussed earlier there are other scenarios in which economic incentives may not lead to adequate security, and insecure supply chains may have serious external impacts on society. On the other hand, the decisions made by society to regulate supply chains to ensure security may have equally serious efficiency and productivity impacts on supply chain firms. It is therefore important that a research and education agenda emphasize the independent perspectives of supply chain firms and society, and their interdependency.

We believe strongly that much of the research required in this area needs to focus squarely on the tradeoffs between supply chain security and supply chain productivity. Initiatives that promote security often increase the complexity of freight handling processes and reduce the efficiency of the freight transportation system and hence the productivity of shippers making use of this system. Balancing security and efficiency is clearly an important goal.

It also appears clear that effective responses to supply chain security threats often require collaborative responses, and therefore research must also consider appropriate collaborative mechanisms for security enhancement. A supply chain is only as secure as its weakest component, and the responsibility for the security of supply chain components often rests with a large number of different firms across many governmental jurisdictions. Clearly, we must research methods for multiple firms (e.g., a group of shippers and a group of carriers) to collaboratively enhance security.

Finally, undoubtedly increased security comes at a price. It is important to analyze the cost-benefit curve associated with efforts targeting increased supply chain security. It is to be expected that initially significant benefits may be achieved at relatively small costs, whereas at some point additional security will come at a relatively large, maybe prohibitively large, costs.

The following four sections, 4.1 through 4.4, describe the compelling research and education themes that we believe should be the focus of the industrial engineering and operations research community.
4.1 Understanding supply chain risk: the perspective of the firm

One of the most fundamental research thrusts is developing an understanding of the risks that threaten to disrupt the normal functioning of global supply chains operated by firms. Determination of appropriate measures of supply chain risk is a crucial goal, and a necessary predecessor to the development of risk-aware supply chains.

A terrorist attack on a seaport is an example of a highly disruptive event that may occur with low probability. In addition to terrorist attacks (or threats of such events) there are many other examples of highly disruptive events occurring infrequently, such as earthquakes, wars, health crisis (e.g., SARS), labor unrests (e.g., U.S. west coast port stevedore strike), hurricanes, floods, major accidents (e.g., a barge ramming a major bridge), business failures, and product recalls. Reviewing this list of disruptive events, it becomes clear that on an individual basis such events may be rare, but overall such events are unfortunately quite common. Therefore, from a research point of view, it is desirable to take a broad and comprehensive perspective on supply chain risk.

Other disruptive events may be more likely, but have lesser impact. A delay at a border (or seaport) as a result of increased security-related inspections is an example of a somewhat disruptive event that may occur with high probability and frequency.

The above examples point to a variety of possible supply chain disruptions as well as to a spectrum of possible supply chain impacts. Consequently, a wide range of approaches to handle security-related disruptions needs to be developed.

4.1.1 Key research challenges

**Metrics.** “If we can measure it, we can control it.” How can supply chain risk be categorized and quantified? What are appropriate methods to measure the likelihood or probability of highly disruptive events? How can we estimate the likelihood of rare events with no historical precedents? How do we measure a supply chain’s vulnerability to disruption? How do we measure a supply chain’s ability to react and recover from highly disruptive events?

4.1.2 References

Sheffi [2001] provides an excellent introduction for understanding supply chain risk, and specifically supply chain risks to terrorist events. Martha and Subbakrishna [2002] also presents an interesting discussion of supply chain risk, and the importance of developing supply chains that are prepared to recover from disruption.
4.2 Design of resilient supply chain systems: the perspective of the firm

A better understanding of supply chain risk and a set of metrics for quantitatively evaluating supply chain risk and supply chain vulnerability may provide insight into the likelihood and consequences of a potential disruption, however it does not prevent disruptions from happening. Therefore, it is essential to include disruption considerations when designing a supply chain. Effective designs minimize the risk of disruption and maximize the ability to quickly recover from a potential disruption. Supply chains that can quickly resume operations after a disruption occurs are called resilient.

Techniques for achieving supply chain resilience include introducing redundancy and building flexibility into designs. Introducing redundancy is a well-known technique for handling variability. Maintaining safety stock inventory, for example, can be viewed as introducing redundancy to handle natural variations in demand. Diversification, in the form of maintaining relationships with multiple suppliers, especially suppliers in different geographical locations, is another way to improve resilience. Postponement, or delayed differentiation, is an adaptive supply chain strategy that enables companies to reduce inventory while improving customer service. However, at the same time, it may also improve supply chain resilience. Maintaining relationships with multiple transportation carriers providing different freight flow paths is another example of diversification that increases the flexibility of the supply chain.

The benefits of supply chain management concepts such as lean management and just-in-time delivery must be weighed and balanced against the resilience of a supply chain. Resilience comes at a cost; building redundancy into a supply chain may lead to high costs. Optimal designs should be developed by developing modeling and solution approaches that consider all appropriate costs and benefits.

Finally, it is important to keep in mind that the design of resilient supply chains not only involves the design of the physical systems, but also includes the design of system management or control strategies.

4.2.1 Key research challenges

Metrics. How does one define resiliency? What are the appropriate metrics to consider when designing resilient supply chains? What metrics should be used to develop a quantitative measure of the resilience of a supply chain? How does one measure the costs of resilience?

Design for resilience. By what means can supply chains become resilient? How can effective flexibility be introduced in supply chains? How can effective diversification be introduced in supply chains? How can effective redundancy be introduced in supply
chains? What will be the effect on productivity, efficiency, and costs? How do these efforts impact modern lean enterprises?

**Risk-aware design.** Can we develop and analyze realistic, tractable optimization models of supply chains that optimize supply chain productivity, given that highly disruptive events may occur with low probability? Such models might take into consideration changes in security inspection protocols due to changes in security threat levels or the use of dual sourcing as a method for enhancing supply chain resiliency.

**Design given preventive measures.** Can we develop and analyze realistic, tractable optimization models of supply chains that optimize expected productivity while complying with new U.S. security initiatives? Can we extend these models to determine the value of asset visibility (perhaps provided or enhanced by RFID technology), the value of offshore security inspections, relative to security inspections at the U.S. entry port, etc.?

**Design for operational response.** Can we develop and analyze realistic, tractable optimization models that design supply chains that can be reconfigured in near-real time when components of the supply chain “fail,” e.g., certain transportation nodes or links are no longer available, certain suppliers are no longer available? Can we develop effective strategies for rerouting freight when certain nodes and/or links unexpectedly lose some or all of their capacity? Can we analyze the economic impact of such events?

**Risk reduction through pooling, outsourcing.** Are there collaborative strategies that allow supply chain risk reduction, e.g., through pooling? How should the costs/benefits of such strategies be shared among collaborative partners? Does outsourcing represent a potential strategy to shift supply chain risks to other supply chain participants?

### 4.2.2 References

4.3 Understanding supply chain infrastructure risk: the perspective of society

Supply chain risks interpreted and perceived by society as a whole might be quite different than those interpreted and perceived by individual firms or even groups of firms. First, certain supply chains may be considered vital for societal well-being; many food supply chains likely fall into this category. For such chains, society may strongly believe that they require protection above-and-beyond what profit-maximizing firms may determine is adequate. Second, all supply chains and in particular international chains create indirect risks to society given their potential for exploitation by malevolent forces.

Supply chains rely heavily on a transportation infrastructure that includes many components that are managed or under government control, such as the interstate highway network, airspace, airports, seaports, and borders. As a result, the government has a responsibility to provide adequate protection to ensure availability and efficiency of the transportation infrastructure. When many firms rely on common infrastructure, such as major seaports, it is clear that disruptions to the operation of such infrastructure may have far-reaching consequences.

4.3.1 Key research challenges

**Metrics.** What are suitable metrics for measuring supply chain infrastructure risk? What are appropriate for measures for quantifying the indirect societal risk posed by supply chains and supporting supply chain infrastructure? How should transportation infrastructure component risks be estimated? How should vulnerability of infrastructure components be measured? Are there appropriate metrics for understanding the importance of certain infrastructure components to supply chain performance, so that appropriate protection prioritization can be made?

**Market response.** Can we develop models to understand and analyze how firms would naturally react to an infrastructure disruption, e.g., to the temporary closure of a seaport? How could such models be used to develop a better understanding of the relative importance of various infrastructure components to overall system vulnerability?

**Impact of prevention measures.** Can we develop analytical approaches that allow quantification of the productivity impacts of transportation infrastructure security measures? For example, can we develop models of supply chain measures that are important to a supply chain manager (e.g., safety inventory level, given a fixed customer service level), as a function of new U.S. security initiative compliance levels (e.g., percentage of containers inspected)?
4.3.2 References

Lewis et al. [2003], Lewis et al. [2004], and Lee and Song [2004] each attempt to address quantification of the productivity impacts of various transportation security processes.

4.4 Design of resilient supply chain infrastructure: the perspective of society

Societies clearly have a role to play in providing protection and prevention mechanisms to reduce the risk of both supply chain disruptions, and the risk of indirect consequences from supply chain exploitation. Many questions may appear quite difficult to analyze quantitatively. At the same time, it is important that crucial societal (and therefore, political) decisions regarding appropriate infrastructure protection mechanisms be made on the basis of strong quantitative analysis.

The design of resilient supply chain infrastructure is especially difficult for two reasons. First, it is important to understand the market response of independent firms to infrastructure changes before making investments in resiliency. As a simple example, suppose a government in an effort to improve the security of major inbound container trade lanes identifies the top few ports exporting containers to the U.S. and implements added security practices at these locations. If the security practices reduce the efficiency of the supply chains using those export ports, profit-maximizing firms may choose to source material from alternative locations that may now provide higher levels of efficiency. In an extreme case, due to market response, a system design that was intended to increase system security might indeed have the opposite effect.

Second, it is likely to be very difficult to develop appropriate measures of the indirect risks of vulnerable supply chain infrastructure. While such indirect risks may indeed be the most important from the perspective of society, they are likely to be the most difficult to quantify and include in analyses. Some guidance and ideas from the hazardous materials transportation and the natural hazards fields, such as earthquake engineering, may be appropriate to consider.

4.4.1 Key research challenges

Metrics. What are the important metrics to consider when designing resilient supply chain infrastructure? How should indirect risks to society be appropriately captured and introduced into models?

Protective measure design. Can quantitative decision models be developed to determine appropriate protective measures for supply chain infrastructure? If protection is to
be achieved via regulation, how should regulations be designed to maximize efficacy and compliance while minimizing efficiency and productivity impacts?

**Collaborative mechanism design.** Mechanism design is the problem of designing a distributed protocol that will implement a particular objective despite the self-interest of individual agents. Can collaborative mechanism design be used to achieve societal goals through various incentives? Can such mechanisms be used to prevent tragedy of the commons?

**Guided response.** Given a disruption of important supply chain infrastructure components, how might a regulatory body enable and efficient and fair coordinated response by supply chain firms? Would such a guided response be desirable from the perspective of society?

4.4.2 References

A number of references may provide the reader with valuable background on societal responses to supply chain security issues. Notable are Stana [2004], Wolfe [2002], and Wolfe [2004]. Wein et al. [2004] describes an interesting research endeavor to use operations research ideas to build effective infrastructure security mechanisms given budget constraints in the context of ocean container security.

5 Information Technology

Since the goal of the workshop was to define basic and applied research challenges for the industrial engineering and operations research community, we have focused primarily on a research agenda that focuses specifically on decision technology research questions. Obviously, there is also a need for extensive investigation into the value of information technology and the required cyberinfrastructure to supply chain security.

As an example, the availability of an electronic supply chain manifest may substantially increase the ability to prevent weaponizing of freight transport vehicles. However, many issues need to be addressed before an electronic supply chain manifest can become a reality., e.g.,

- chain of custody/chain of possession,
- institutional/legal issues in sharing data (who has access to materials? what are their credentials?),
- an international standard for electronic data interchanges is required (how to handle the various languages?)
It is equally important to investigate the value of new technologies such as RFID, smart seals, e-seals, etc.

**Acknowledgements**

This work was supported by National Science Foundation grant DMII\#0334492, the Sloan Foundation Trucking Industry Program, and The Logistics Institute–Asia Pacific. The Georgia Institute of Technology and The Logistics Institute provided additional support for the workshop described herein.

**References**


## APPENDIX A
### WORKSHOP AGENDA

### Tentative Schedule

#### February 4, 2004

<table>
<thead>
<tr>
<th>Time</th>
<th>Event</th>
</tr>
</thead>
<tbody>
<tr>
<td>8:30-9:00am</td>
<td>Welcoming Remarks and Introductions</td>
</tr>
<tr>
<td>9:00-10:00am</td>
<td><strong>Session: The Government Perspective</strong></td>
</tr>
<tr>
<td></td>
<td>Randy Butler, <em>U.S. DoT</em></td>
</tr>
<tr>
<td></td>
<td>Bud Hunt, <em>TSA</em></td>
</tr>
<tr>
<td></td>
<td>John Holmes, <em>SAIC</em></td>
</tr>
<tr>
<td>10:00-10:30am</td>
<td>Break</td>
</tr>
<tr>
<td>10:30-11:30am</td>
<td><strong>Panel: The User's Perspective</strong></td>
</tr>
<tr>
<td></td>
<td>Jim Kellso, <em>Intel</em></td>
</tr>
<tr>
<td></td>
<td>Londndon Seely, <em>The Home Depot</em></td>
</tr>
<tr>
<td></td>
<td>Jeff Tew, <em>General Motors</em></td>
</tr>
<tr>
<td>11:30-12:30pm</td>
<td><strong>Buffet Lunch</strong> (Georgia Tech Hotel Dining Room)</td>
</tr>
<tr>
<td>12:30-1:15pm</td>
<td>Presentation by Stephen Flynn, <em>Council on Foreign Relations</em> and former <em>Coast Guard</em></td>
</tr>
<tr>
<td>1:30-2:30pm</td>
<td><strong>Panel: The Provider's Perspective</strong></td>
</tr>
<tr>
<td></td>
<td>Dan Davis, <em>BAX Global</em></td>
</tr>
<tr>
<td></td>
<td>Pam Everitt, <em>Port of Charleston</em></td>
</tr>
<tr>
<td></td>
<td>Steven Kretsch, <em>Stolt-Nielsen</em></td>
</tr>
<tr>
<td></td>
<td>Richard Duncan, <em>Hartsfield-Jackson Atlanta International Airport</em></td>
</tr>
<tr>
<td>2:30-2:45pm</td>
<td>Break</td>
</tr>
<tr>
<td>2:45-3:15pm</td>
<td>Presentation by Prof. Chip White, <em>GT – Security and Efficiency in Transportation</em></td>
</tr>
<tr>
<td>3:15-3:45pm</td>
<td>Presentation by Prof. Randy Hall, <em>USC – Homeland Security Center</em></td>
</tr>
<tr>
<td>3:45-4:00pm</td>
<td>Break</td>
</tr>
<tr>
<td>4:00-5:30pm</td>
<td><strong>Breakout Sessions</strong></td>
</tr>
<tr>
<td></td>
<td>Room 330/331 in Georgia Tech Global Learning and Conference Center</td>
</tr>
<tr>
<td>5:30-6:15pm</td>
<td>Cocktails (Georgia Tech Hotel, Corner space of 5th St. and Spring, 2nd Floor)</td>
</tr>
<tr>
<td>6:30-8:00pm</td>
<td>Dinner (Georgia Tech Hotel, Conference Room E)</td>
</tr>
</tbody>
</table>

#### February 5, 2004

<table>
<thead>
<tr>
<th>Time</th>
<th>Event</th>
</tr>
</thead>
<tbody>
<tr>
<td>8:00-9:00am</td>
<td>Continental Breakfast (Georgia Tech Global Learning and Conference Center)</td>
</tr>
<tr>
<td>9:00-10:00am</td>
<td><strong>Reports from Breakout Sessions</strong></td>
</tr>
<tr>
<td></td>
<td>Moderator: Chip White, Georgia Tech</td>
</tr>
<tr>
<td>10:00-10:30am</td>
<td>Break</td>
</tr>
<tr>
<td>10:30-11:30am</td>
<td>Presentation by Prof. Yossi Sheffi, <em>MIT-Homeland and Global Security</em></td>
</tr>
<tr>
<td>11:30-12:00pm</td>
<td><strong>Closing Session and Adjourn</strong></td>
</tr>
<tr>
<td>12:00-1:00pm</td>
<td><strong>Buffet Lunch</strong> (Georgia Tech Hotel Dining Room)</td>
</tr>
</tbody>
</table>
APPENDIX B

NSF Workshop on Supply Chain Security and Productivity:
Research and Education Implications
February 4-5, 2004

Georgia Tech Global Learning and Conference Center -- Atlanta, GA

Attendee Roster

Dr. Michael Ball
Professor
University of Maryland
Robert H. Smith School of Business
College Park, MD  20742
P: 301-405-2227
F: 301-405-8655
Email: mball@rhsmith.umd.edu

Ms. Caroline Beaird
International Supply Chain Analyst
The Home Depot
Store Support Center C-15
2455 Paces Ferry Road
Atlanta, GA  30339
P: 770-433-8211 x83412
F: 770-384 2758
Email: caroline_beaird@homedepot.com

Mr. Randy Butler
Transportation Specialist
FHWA
HOFM-1 Room 3401
400 Seventh Street, SW
Washington, DC 20590
P: 202-366 9215
F: 202-366 7909
Email: randy.butler@fhwa.dot.gov

Dr. Robert Cook
Yamacraw Professor
Georgia Southern University
Dept. of Computer Sciences #7997
Georgia Southern University
Statesboro, GA  30460
P: 912-681-0892
F: 912-486-7672
Email: bobcook@georgiasouthern.edu

Mr. Dan Davis
Manager, Corporate Security
BAX Global
One Air Cargo Parkway East
Swanton, OH 43558
P: 419-867-9914
F: 419-491-1019
Email: davis@baxglobal.com

Mr. Richard Duncan
Email: richard.duncan@atlanta-airport.com

Ms. Debra Elkins
Senior Research Engineer
General Motors R&D
Mailcode 480-106-359, 30500 Mound Road
Warren, MI  48090-9055
P: 586-986-2750
F: 586-986-0574
Email: debra.elkins@gm.com

Ms. Pam Everitt
Director Information Technology
SC State Ports Authority
176 Concord Street
Charleston, SC  29401
P: 843-577-8678
F: 843-577-8710
Email: peveritt@scspa.com

Dr. Randolph Hall
Senior Associate Dean for Research
University of Southern California
240 GER, Epstein Department of Industrial
& Systems Engineering, USC
Los Angeles, CA 90089-0193
P: 213-740-4894
F: 213-740-1120
Email: rwhall@usc.edu
Ms. Kathryn Harrington-Hughes
Vice President
Eno Transportation Foundation
1634 I St. NW, Suite 500
Washington, DC 20006
P: 202-879-4718
F: 202-879-4719
Email: khh@enotrans.com

Mr. John Holmes
Vice President, Director of Port Business Development
Science Applications Int’l Corporation
595 W. 7th St., Suite 201
San Pedro, CA 90731
P: 310-732-5992
F: 310-832-7428
Email: john.m.holmes@saic.com

Mr. Walter (Bud) Hunt
Chief, Maritime Cargo Security Branch
TSA, Maritime and Land Security
TSA Headquarters - East Building
10th Floor, TSA-8
601 South 12th Street, VA 22202-4220
P: 571-227-2152
F: 571-227-1923
Email: bud.hunt@dhs.gov

Dr. Phil Kaminsky
Associate Professor
UC Berkeley
IEOR Department
4141 Etcheverry Hall # 1777
Berkeley, CA 94720-1777
P: 510-642-4927
F: 510-642-1403
Email: kaminsky@ieor.berkeley.edu

Mr. James Kello
Manager of Supply Network Research
Intel Corporation
6505 West Chandler Ave CH11- 121
Chandler, AZ 85226
P: 480-554-8715
F: 480-552-2400
Email: jim.r.kello@intel.com

Mr. Steven Kretsch
Director
Stolt-Nielsen Transportation Group
8 Sound Shore Drive
Greenwich, CT 06836
P: 203-625-3821
F: 203-625-3552
Email: skretsch@sntg.com

Mr. Hani Mahmassani
Professor and Director
University of Maryland
Maryland Transportation Initiative
1173 Martin Hall
College Park, MD 20742
P: 301-405-0752
F: 301-405-2585
Email: masmah@mail.umd.edu

Mr. Jim Newsome
Senior Vice President
Hapag-Lloyd (America), Inc
245 TownPark Drive
Kennesaw, GA 30144
P: 678-355-6500
F: 770-419-1857
Email: jim.newsome@hlcl.com

Ms. Gail Pesyna
Program Director
Alfred P. Sloan Foundation
630 Fifth Avenue, Suite 2550
New York, NY 10111
P: 212-649-1649
F: 212-757-5117
Email: pesyna@sloan.org

Mr. Ronald Rardin
Professor of Industrial Engineering
Purdue University
Potter Center, Room 316
West Lafayette, IN 47907-2022
P: 765-494-5410
F: 765-494-2351
Email: rardin@purdue.edu
Ms. Lonndon Seely  
Director, Global Logistics Asset Protection  
The Home Depot  
2455 Paces Ferry Road, N.W.  
Atlanta, GA  30339  
P: 770-384-4587  
F: 770-384-3013  
Email: lonndon_seely@homedepot.com

Dr. Suvrajeet Sen  
Program Director  
National Science Foundation  
4201 Wilson Blvd  
Arlington, VA  22230  
P: 703-292-7081  
F: 703-292-9056  
Email: ssen@nsf.gov

Dr. Yossi Sheffi  
Professor  
MIT  
Room E40-275, MIT  
77 Mass Ave.  
Cambridge, MA 02139  
P: 617-253-5316  
F: 617-253-8496  
Email: sheffi@mit.edu

Mr. Jeffrey Short  
Research Associate  
American Transportation Research Institute  
1800 Lake Park Drive  
Suite 123  
Smyrna, GA 30080  
P: 770-432-0628  
F: 770-432-0638  
Email: jshort@trucking.org

Mr. Jeff Tew  
Technical Fellow, Group Manager for  
    Manufacturing Enterprise Modeling  
General Motors R & D Center  
Mailcode 480-106-359, 30500 Mound Road  
Warren, MI  48090-9055  
P: 586-986-7926  
F: 586-986-0574  
Email: jeffrey.tew@gm.com

Dr. Reha Uzsoy  
Director, Laboratory for Extended Enterprises  
Purdue University  
School of Industrial Engineering  
West Lafayette, IN 47907-1287  
P: 765 4940829  
F: 765 4940829  
Email: uzsoy@ecn.purdue.edu
Georgia Tech:

Dr. John Bartholdi
Manhattan Associates Professor of Supply Chain Management
Research Director, TLI
School of Industrial and Systems Engineering
Georgia Tech
765 Ferst Drive NW
Atlanta, GA 30332-0205
P: 404-894-3036
F: 404-894-2301
Email: john.bartholdi@isye.gatech.edu

Dr. Mokhtar Bazaraa
Managing Director, Global Logistics, TLI
School of Industrial and Systems Engineering
Georgia Tech
765 Ferst Drive NW
Atlanta, GA 30332-0205
P: 404-894-4821
F: 404-894-0390
Email: mo.bazaraa@isye.gatech.edu

Ms. Carole Bennett
Director
Program Development and Marketing, TLI
School of Industrial and Systems Engineering
Georgia Tech
765 Ferst Drive NW
Atlanta, GA 30332-0205
P: 404-894-9138
F: 404-894-6527
Email: carole.bennett@isye.gatech.edu

Mr. Harvey Donaldson
Director, The Logistics Institute
School of Industrial and Systems Engineering
Georgia Tech
765 Ferst Drive NW
Atlanta, GA 30332-0205
P: 404-894-2343
F: 404-894-6527
Email: harvey.donaldson@isye.gatech.edu

Dr. Alan Erera
Assistant Professor
School of Industrial and Systems Engineering
Georgia Tech
765 Ferst Drive NW
Atlanta, GA 30332-0205
P: 404-385-0358
F: 404-894-2301
Email: alan.erera@isye.gatech.edu

Dr. Marc Goetschalckx
Associate Professor
School of Industrial and Systems Engineering
Georgia Tech
765 Ferst Drive NW
Atlanta, GA 30332-0205
P: 404-894-2317
F: 404-894-2301
Email: marc.goetschalckx@isye.gatech.edu

Dr. Pinar Keskinocak
Assistant Professor
School of Industrial and Systems Engineering
Georgia Tech
765 Ferst Drive NW
Atlanta, GA 30332-0205
P: 404-894-2325
F: 404-894-2301
Email: pinar.keskinocak@isye.gatech.edu

Dr. Anton Kleywegt
Assistant Professor
School of Industrial and Systems Engineering
Georgia Tech
765 Ferst Drive NW
Atlanta, GA 30332-0205
P: 404-894-4323
F: 404-894-2301
Email: anton.kleywegt@isye.gatech.edu

Dr. C. John Langley, Jr.
The Logistics Institute Professor of Supply Chain Management
Director, Supply Chain Executive Forum
Georgia Tech
765 Ferst Drive NW
Atlanta, GA 30332-0205
P: 404-894-6523
F: 413-556-3570
Email: john.langley@isye.gatech.edu
Did not attend:

Mr. Aaron Lukas  
Analyst, Center for Trade Policy Studies  
Cato Institute  
1000 Massachusetts Ave., NW  
Washington, DC  20001  
P: 202-789-5271  
Email: alukas@cato.org

Email addresses:  
mball@rhsmith.umd.edu;  
caroline_beaird@homedeport.com;  
randy.butler@fhwa.dot.gov;  
obocoook@georgiasouthern.edu;  
ddavis@baxglobal.com;  
richard.duncan@atlanta-airport.com;  
debra.elkins@gm.com;  
peveritt@scspa.com;  
rwhall@usc.edu;  
john.m.holmes@saic.com;  
khh@enotrans.com;  
Bud.Hunt@dhs.gov;  
kaminsky@ieor.berkeley.edu;  
jim.r.kelso@intel.com;  
skretscht@sntg.com;  
alukas@cato.org;  
pesyna@sloan.org;  
masmah@mail.umd.edu;  
jim.newsome@hlcl.com;  
rardin@purdue.edu;  
lonndon_seely@homedeport.com;  
ssen@nsf.gov;  
sheffi@mit.edu;  
jshort@trucking.org;  
jeffrey.tew@gm.com;  
uzsoy@ecn.purdue.edu