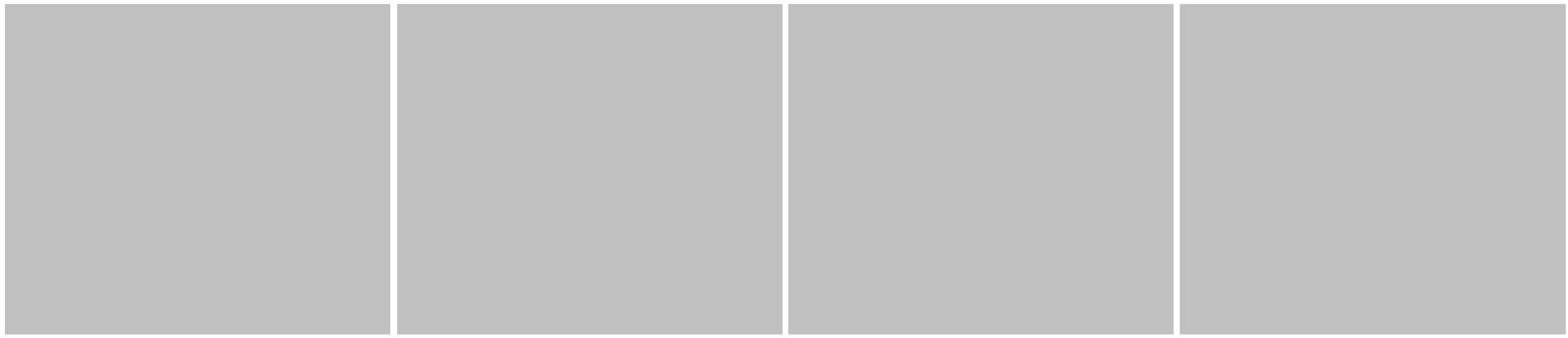
IBM Business Consulting Services

November 2005

Global Movement Management: Securing the Global Economy



W. Scott Gould, Vice President, Public Sector Strategy & Change, IBM
Christian Beckner, Senior Consultant, Public Sector Strategy & Change, IBM

Executive Summary

The global movement system is the engine of global prosperity today. Economic integration and improvements in system efficiency have created a single global economy, but one whose very strengths – speed, openness, and efficiency – put it at risk of disruption from external threats. There have always been threats to the global movement system, but the attacks of 9/11 provided a paradigm shift in the potential severity and nature of these threats. This new and greater threat creates the need for a comprehensive framework for securing the system: Global Movement Management.

Global Movement Management (GMM) is a comprehensive and achievable framework for securing the key flows – people, goods, conveyances, money, and information – in the global economy against disruptive threats and building resiliency into the system. The framework is aligned with the existing commercial imperatives of the global system and the protection of important societal values such as privacy and civil liberties. The framework consists of two conceptual parts: a governance structure and a system architecture.

Numerous steps have been taken to improve the security of the global movement system since 9/11, but these have been largely piecemeal. Many efforts have stalled due to an uncertain governance structure, both among nations and between the public and private sectors. Key stakeholders have been hesitant to adopt new security measures, uncertain of their potential impact on commerce, or on privacy and data protection. The Global Movement Management framework meets these challenges by proposing a governance structure that is distributed and decentralized, using rules, standards, and market-driven incentives to encourage investment in the security and resilience of the system.

Global Movement Management is an integrated framework that looks holistically at the key variables in the system – flows, locations, modes of transport and exchange, and time – and finds areas of convergence across the existing system that are building blocks for enhancing security. These include: (a) common security and business functions, (b) existing borders and checkpoints, (c) existing data sources and information flows, and (d) existing relationships among key system participants. These system elements can be woven together to form a common system architecture – one that is flexible, adaptable, and largely decentralized, with the exception of a core set of seamless and closely controlled security applications.

This Global Movement Management framework can help overcome the key impediments to efforts to promote security in the global movement system, and motivate key stakeholders to work together to integrate security and resilience into the system. It can protect and strengthen the common foundations of global interconnectedness and prosperity.

I. The Global System Today

The global economy of the 21st century is built upon a foundation of openness and mobility. Goods are shipped across oceans and continents, and delivered to consumers with efficiency and breakneck speed. People can travel by plane to the far corners of the world in a matter of hours. Information moves instantly around the world via the Internet and the global communications grid, connecting people and nations. Money flows across borders just as quickly through the global financial system by means of electronic transactions. Business is conducted collaboratively and virtually on a global basis.

All of these flows – of people, goods, conveyances, money, and information – are the connective tissue of globalization, and the foundation upon which the global economy is able to endure and grow. The system is the result of successive waves of innovation in the 20th century – built on technologies such as flight, containerized shipping, ground transport, telecommunications, computing, and the Internet. As a result, the global economy is interconnected today to a degree that is unprecedented in human history.

But this interconnectedness creates new risks. The impacts of negative events, such as a hurricane or earthquake in the United States, a terrorist attack in Europe, or the outbreak of an infectious disease in Asia, are no longer isolated, but can ripple through the system and have a profound and multiplying disruptive effect around the world. And various types of bad actors – rogue states, drug cartels, organized crime syndicates, or terrorist groups – can exploit the system's openness and anonymity to facilitate their illicit and harmful activities. Criminals, fanatics, and terrorists no longer need to leave the isolation of the basement or the cave to conduct their business on a global scale.[1] The system's core strengths – its performance, speed, efficiency, interconnectedness, precision, and predictability – are also now sources of systemic risk and vulnerability. One of the most important challenges that leaders in the public and private sector currently face is finding new ways to strengthen this system in an evolving political environment, and protecting it from the buffeting forces of external disruption and misuse.

The terrorist attacks of 9/11 exposed the intrinsic fragility of this system and the need for greater security within it. The global economic system has always been at the risk of misuse, but after 9/11, the known risks are different. The threat of large-scale terrorism or rogue state aggression involving weapons of mass destruction poses an existential threat to the civilized world – and puts the global system at the risk of massive disruption or total breakdown.

There are two important aspects to the threat as it specifically pertains to the global economic system. First, the system itself is a target. One of al-Qaeda's[2] key tactical objectives is to undermine the economies of the Western world. The attacks of 9/11 were directly aimed at the commercial aviation system and the financial, political, and military nerve centers in New York and Washington. But they were also collaterally targeted at the global economy itself. In a video released in April 2002, Osama Bin Laden famously joked with his cohorts about $640 billion in short-term lost value on the stock market as a result of 9/11. In November 2004, he boasted that for every single dollar that al-Qaeda was spending on insurgency in Iraq, the United States was spending $1 million there to combat the insurgency. This kind of economic calculus is a

[1] The geographic footprint of the terrorist attacks of 9/11 are the most notable example of this globalization of terror – the planning and recruitment for the attacks took place in at least 11 countries around the world, including Afghanistan, Czech Republic, Egypt, Germany, Lebanon, Malaysia, Pakistan, Saudi Arabia, Spain, United Arab Emirates, and the United States.

[2] Al-Qaeda is referenced here rather than all terrorist groups, because the group's millenarian intentions far surpass those of any other major terrorist group today. But it is probable that future terrorist groups – ones which do not exist today – will emulate al-Qaeda's intentions and match or surpass its capabilities.

critical element of al-Qaeda's strategy of asymmetric force and is likely to inform its future goals and activities.

Second, the terrorist threat operates inside of the broader global economic system, and terrorists use its capabilities to move people, goods, conveyances, information, and money in support of their operations. The attacks of 9/11 were carried out **within and through** the global economic system. The terrorists involved in planning and carrying out the attacks leveraged the global economic system to maximize their opportunity for success and multiply the effects of the attacks. They exploited gaps and flaws in visa and entry systems to get attackers and their support networks into a country. They understood the operational imperatives of the aviation industry, and chose specific flights that would maximize their probability of success. They compartmentalized their operations, reducing the vulnerability that the capture or exposure of one person or one cell would expose the entire plot. They used the global financial system to acquire the funds necessary to carry out the attacks. Essentially, the terrorists were able to create their own "terrorist supply chain" and "terrorist travel system" within the broader system. Since 9/11, terrorist groups have continued to develop their capabilities to exploit the system, using the Internet to disseminate information, raise funds, and conduct recruiting.

These two aspects contribute to the need for a new framework to secure the global economic system: one that is aligned with the existing and complex realities of the system, but recognizes the paradigm shift in the nature of threat that it faces today. We call this framework **Global Movement Management.**

II. Global Movement Management Defined

Global Movement Management (GMM) is a comprehensive and achievable framework for securing the key flows – people, goods, conveyances, money, and information – in the global economy against disruptive threats and for building resiliency into the system. It is a framework that sustains and protects the core strengths of the current global system – its performance, speed, efficiency, interconnectedness, precision, and predictability – and adds two new system imperatives: security and resilience. It is a framework that recognizes and protects core societal values such as privacy and civil liberties. **Security** means protecting the system from being disrupted or attacked, or exploited as a means of carrying out or planning an attack. **Resilience** means ensuring that the system can minimize the impacts of a disruption and recover easily from its direct or secondary effects.

Efforts to secure and build resilience into the global economic system are not new, and have antecedents that are hundreds of years old, in the form of efforts to protect nations and commerce against the threats of piracy, foreign infiltration, and commercial fraud. Since 9/11, many measures have been taken around the world to respond to these new imperatives and develop security for each of the five system flows, including:

- **People:** Numerous efforts to improve security at national border checkpoints, including the Schengen Information System, US-VISIT, and the Australian Advanced Passenger Processing System. Remote border area security initiatives such as the planned America's Shield Initiative (ASI). Passport, visa, and identification issuance systems in dozens of countries around the world, the supporting architecture for credentialing, checking backgrounds, and watch-listing people, and the International Civil Aviation Organization (ICAO) Machine Readable Travel Documents (MRTD) standards for these forms of identification. Passenger

screening systems, both physical (e.g., explosive detection equipment, metal detectors for the commercial aviation system and rail systems) and informational (e.g., Secure Flight in the United States, Project Semaphore in the United Kingdom).

- **Goods:** Measures to certify cargo at the point of loading or embarkation (the Customs Trade Partnership against Terrorism (C-TPAT)), screen it at points of departure or other system chokepoints (the Container Security Initiative (CSI) and Megaports Initiative in the United States), track it across the supply chain, and certify it before its arrival into a country such as through the Advance Manifest Rules implemented by Canada, the European Union, and the United States.
- **Conveyances:** Efforts to track the conveyances, including planes, ships, trains, and trucks that move cargo around the world, whether at sea (Maritime Domain Awareness), or in the air (Air Traffic Control modernization), or on land (GPS-based truck-tracking systems).
- **Money:** Initiatives aimed at disrupting terrorism-related finances and money laundering, led by groups such as the international Financial Action Task Force (FATF) and agencies such as FINTRAC in Canada, the Terrorist Finance Unit in the United Kingdom, and FinCEN and OFAC in the United States.
- **Information:** Measures aimed at monitoring and disrupting the communications of terrorist cells and related groups, through channels such as e-mail, chat room communications, telephony, and mail and courier services.

There have also been a range of efforts undertaken to improve the physical and cybersecurity of the fixed assets of the global movement system, including airports, seaports, transportation centers and bottlenecks, border checkpoints, and major network hubs.

All of these initiatives and efforts contribute to security and system resilience, and deter terrorists and other bad actors from carrying out attacks within it. But they are today a collection of tactics, not guided by a coherent and overarching strategy. In the absence of such a strategy, the system is suboptimized in a number of ways. Governments lack the ability to make informed decisions about priorities among competing missions and needs. Private sector stakeholders are unable or unwilling to take the first move and invest their own resources. The risk of security gaps in the system is unnecessarily high. Potential system synergies and efficiencies cannot be easily created.

To understand why a true strategy for securing the global economic system has not emerged, we need to look at four challenges within the system today.

III. Challenges to a Strategic Approach

There are four key challenges to adopting a strategy that promotes security and resilience in the system today:

1. Integration of security and resilience with the commercial imperatives of the system.
2. Integration of security and resilience with societal imperatives such as privacy and civil liberties.
3. International cooperation and harmonization.
4. Cooperation between the public sector and the private sector.

A Global Movement Management framework enables the system to overcome these challenges through its two most important elements: a governance structure and a system architecture.

These are detailed in later sections of this report. Before that, it is necessary to look in detail at these systemic challenges.

The first critical challenge is **integrating security and resilience with the commercial imperatives of the system**, including speed, performance, efficiency, interconnectedness, and predictability. Any new security-related activity will be more readily adopted if it enhances the performance and efficiency of the system, and will be resisted if it degrades that performance. The key private sector stakeholders in the system are likely to fund security investments only if they deliver concrete benefits beyond the often intangible benefits of security and resilience. If a good security concept is flawed in execution and harms the stakeholders who are responsible for implementing it on a day-to-day basis, then it will not be used – a worse outcome than having no security at all. Ultimately, security and resilience need to become embedded into these broader system imperatives, creating a culture of "Total Security Management," in a manner similar to the drive for "Total Quality Management" in manufacturing, or the growth of safety as a paramount engineering norm in the aviation system and in automotive design.

A second critical challenge derives from the existence of national laws and standards for **privacy, data protection, and civil liberties**. Privacy is a critically important civil and personal right around the world, and often leads to the creation of legal and regulatory constraints on the collection and use of personal and other sensitive information. There are good reasons why certain activity should be regulated and constrained, but it is often challenging to define where the line should be drawn, and for which activities the benefits of security outweigh the losses of privacy and personal freedom. Compounding this challenge is the fact that privacy means different things to different societies. For example, in Europe, privacy is a fundamental right protected by cross-sectoral laws that apply to both the public and private sectors, and Europeans seem more comfortable sharing information with the government than with the private sector. In the United States, the opposite is true, and people are generally more wary about use of personal information by the government. Several existing frameworks and policies are applicable to cross-border transfers of personally-identifiable information,[3] and need to be reconciled with the new security imperatives of the system. Civil liberties issues also sometimes pose a challenge to a strategic approach, in cases where societal norms such as non-discrimination and the right to due process might clash with the operational performance of some types of security activities, such as personal profiling in aviation screening or the detention and removal of illegal aliens.

A third critical challenge is **international cooperation**, and finding ways to overcome and resolve the disparate interests among sovereign national governments in the GMM system. Governments are wary of sharing information about their citizens with other nations, especially in cases where safeguards are not in place or countries have different attitudes about where to strike the balance between privacy and security. Also, governments may have different perceptions of the terrorist threat, and thus may choose security investments that are optimal from a national perspective, but suboptimal from a global perspective. For example, a country in Europe that believes it is at low risk for terrorism could make only small investments in counter-terrorism, and create a permissive environment for groups that might carry out attacks on a broader international basis. The GMM system is intended to overcome the consequences of these disparate interests, and create a framework that aligns the interests of stakeholders and supports optimal participation by each country while allowing different policy choices.

[3] Such as the OECD's Guidelines on the Protection of Privacy and Transborder Flows of Personal Data

A fourth critical challenge is **cooperation between public sector and private sector stakeholders**. The Global Movement Management system is largely a privately-owned and operated system, and private sector stakeholders understand the intricacies of the system better than any bureaucracy. But national governments understand the threat of terrorism much better than any private company, and are in the best position to assess risk at the macro-level and establish priorities about how to secure the system. This imbalance of information between private sector domain knowledge and public sector threat-related knowledge means that no single party has the ability to operate solely on its own, and it creates uncertainty about how to distribute and share the costs of upgrading security and resilience in the system,

Taken together, these four challenges pose a formidable barrier to the implementation of a coherent and effective security and resilience strategy for the global economic system. The complexity and heterogeneity of the system make it difficult to move forward strategically, which is why activity to date has been tactical and bite-sized. What is needed to overcome this barrier is a framework that distills the current system's complexity and heterogeneity to its essential elements, and uses this understanding of the system to propose a governance structure and system architecture that can enhance security and resilience in the entire system: a framework of Global Movement Management.

IV. Building A GMM Framework

Given the scope and scale of the global economic system, establishing a GMM framework is a daunting task. But the system can be made comprehensible by breaking it down to its essential parts, and looking at it from a modular and decentralized perspective. This perspective makes it possible to proceed step-by-step, and use a spiral development approach to integrate new activities into the existing system – in a way that is coordinated in its design and delivers the level of security and resilience that the system needs, while at the same time maintaining or improving the commercial and privacy-related imperatives of the system.

The establishment of this framework is a four-step process:

1. Analyze the current system to reveal its key building blocks.
2. Use these building blocks to construct a clear picture of security- and resilience-relevant linkages and commonalities across the current system.
3. Develop a governance structure on the basis of this system picture that can enable and manage GMM activities.
4. Develop a common architecture for Global Movement Management that defines the basic requirements for human and technical capabilities needed to build the system of systems.

These four steps – moving from an analysis of the parts of the system, through a synthesis of common attributes, to the proposal of a governance structure and system architecture – are discussed in detail in the remainder of **Section IV** as well as **Sections V and VI**.

A. Analyzing the Global Economic System

The global economic system can be broken down along multiple dimensions. By analyzing the system and attempting to find patterns in its complexity, we can develop a strategy to manage security and resilience within it. Within a broader set of system dimensions and attributes (including efficiency, performance, cost, and identity), the five most relevant of these as they pertain to security and resilience are flow type, location, custody, mode of transportation and exchange, and time, as follows:

1. **Flow type:** The first dimension of the system is what is moving through it. The five main flow types in the system, as identified earlier, are people, cargo, conveyances, information, and money.[4]

2. **Location:** The second dimension is the location where something is taking place. This can be looked at generically, such as internal to a country, at a border, or in a foreign country; or specifically, examining the critical differences among key countries (by things like national motivations, political frameworks, and resources) in the system.

3. **Custody:** The third dimension is who or what is in control and/or ownership of what is moving through the system. This includes both custody in a formal, legal sense (e.g., cargo moving through the supply chain) and in a less formal sense (e.g., passengers on an airplane or in a border queue).

4. **Mode of transport or exchange:** The fourth dimension is the mode of transport and/or the mode of exchange. For people and goods, key modes of transport include air, sea (including ships and inland barges), and land (including cars, trucks, and rail).[5] For money and information, important modes of exchange include telephony systems, the Internet, satellite-based communications systems, narrow-range communications technologies, including, for example, RFID and Bluetooth, and financial payment and settlement systems.

5. **Time:** The fifth dimension of the system is the factor of time. Some transactions and interactions within the system are instantaneous; others are bound by the physical realities of the global transport system. In some parts of the system, it is possible today to have real-time situational awareness about the system state; in other parts, this awareness does not yet exist (and might be difficult to create).

B. System Commonalities and Linkages

Looking closely at the system along these five dimensions, a number of trends and commonalities start to emerge. System activities that had seemed unrelated reveal their linkages and commonalities. Patterns of human, physical, and informational interaction become self-evident. System activities that had no obvious connection to security or resilience reveal their potential utility for advancing these imperatives.

Ultimately, four types of commonalities and linkages emerge:

1. Common security and resilience-related **business functions**.
2. Common **control points**, including national borders, movement chokepoints, and physical infrastructure.
3. Existing **data sources**, transactions, and information flows that can provide inputs into the system.
4. Relationships among key system **stakeholders**.

These four commonalities and linkages are the baseline building blocks of the GMM framework, and are discussed in the following four sections. They provide the leaders responsible for

[4] Some of these flows are both objects and agents of the global system; that is, as agents they also facilitate the movement of other flows within the system. For example, activities and transactions involving people, money, conveyances, and information are all necessary in order to move goods through the system.

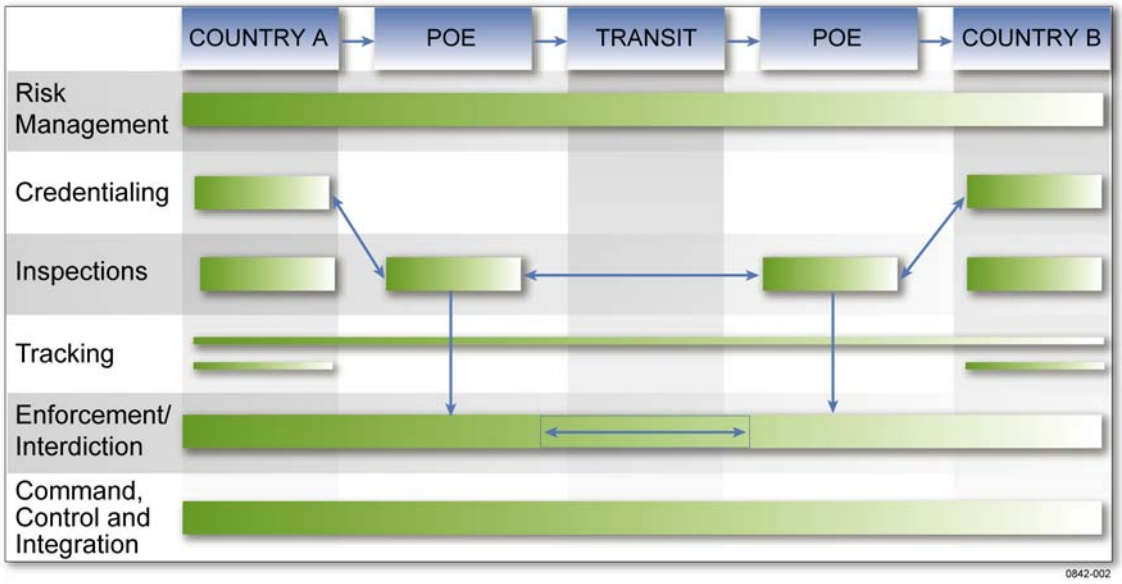
[5] These modes of transport are the same thing as the "conveyances" flow. But we treat it in this paper in two distinct places because conveyance-centric security is a security alternative distinct from the people or goods that conveyances carry.

building security and resilience into the system with information on what they have to work with today, and what they need to create to plug gaps and weave together the system. The sections below describe each of these four types of commonalities and linkages in detail.

1. Security and Resilience-Related Business Functions in the GMM Framework

In terms of security and resilience activities in the global economic systems, there are six overarching business functions that cut across flow, location, mode, and time. These functions are: (1) risk management, (2) credentialing, (3) screening and inspections, (4) tracking, (5) enforcement and interdiction, and (6) command, control and integration (CCI). Chart I plots the business functions on the vertical axis against generic location types on the horizontal axis, with respect to multiple flows in the system.

Chart I: Security And Resilience Business Functions



Risk management is the collection and analysis of data about many different types of flows – such as people, cargo, and financial transactions – to identify the level of risk for a given entity. Risk management processes information in the aggregate, illuminating anomalies and identifying otherwise imperceptible threats. Most importantly, risk management programs facilitate efficient resource management and the expedited movement of low-risk people and cargo (the vast majority of the flow), focusing limited resources on the entities that pose the highest risk.

Credentialing is the business function that asserts that at a given point in time, people are who they claim to be and/or that the conditions of those types of flows (e.g., people, cargo, data sources, financial transactions) meet a certain standard. Generally, credentials are issued at points of surety, where a credentialing authority is convinced that certain standards have been met. These credentials are used at later points in time to help validate claims of identity, content, or other conditions. In the event that the integrity of an identity or shipping credential is determined to be intact, any information related to the individual, cargo, or shipper can be used more effectively to manage risk and allocate inspection resources appropriately. Credentialing increasingly follows a model of registering trusted and authorized frequent users

of a system and pre-clearing them, such as the piloted Registered Traveler programs in the United States; the Border Crossing Card programs involving Canada, Mexico, and the United States (FAST, SENTRI, NEXUS); and the Customs Trade Partnership against Terrorism within the physical supply chain. These are tied internationally to emerging standards for mutual recognition of credentials, such as the WCO Framework v2.0 or EU Customs 2007.

Screening and inspection includes business functions that conduct inspection and accounting activities to verify that flows that cross national borders or move through a chain of custody are properly identified and registered. Screening and inspection helps to validate that only lawful or low risk people or things enter intentional openings in perimeter boundaries such as ports of entry and that authorities are able to track the duration of their stay within those boundaries effectively. It is used throughout the supply chain to allocate additional inspection and/or enforcement and interdiction resources, and it informs compliance programs such as warnings, training, audits, and facilitation programs. Screening and inspection is highly dependent upon risk assessment to gauge the risk of the targets of inspection.

Tracking includes business functions that monitor and track people, cargo, conveyances, or transactions that have entered or intend to enter perimeter boundaries lawfully. It includes processes and systems to track people, cargo, conveyances, and money to validate that their location and integrity is consistent with that authorized upon entry. It includes the process of attributing the ownership and control of items moving through the system. It includes traceability processes: tracking backward to find the source or origin of a system disruption (e.g., poultry infected with avian flu or WMD materials intercepted in a cargo container), isolating the problem and thus decreasing the need for a broad system shutdown. Tracking is typically non-intrusive and the information from this business function can be aggregated to create a comprehensive real-time picture of the state of the system, which can be used both for security functions and business efficiency functions (e.g., inventory management, optimizing use of assets). Many of today's legacy tracking systems are immature and unable to track flows moving across borders or chains of custody.

Enforcement and interdiction facilitates the integrity of a country's borders and interdicts illicit activity within countries. It includes enforcement of the law at and between lawful ports of entry, identifies breaches in the perimeter, and takes action to prevent entry of illegal immigrants or unauthorized cargo, including weapons of mass destruction. It includes the ability to respond effectively to changes in the at-entry conditions of people, cargo, and conveyances. Finally, it includes interior enforcement activities, including the detention and removal of illegal entrants and investigations into the smuggling of terror-related or other illicit substances.

Command, control and integration (CCI) includes net-centric command and control activities (involving both the public and private sectors) that monitor all available information about global movement, and fuse that information to create real-time intelligence about potential threats to the system, in a manner consistent with privacy and civil liberties standards. It supports efforts across all of the business functions to share and analyze data more effectively, particularly from risk assessment, and it optimizes enforcement and interdiction response times and effectiveness.

These six business processes in the global movement system interact with each other and with multiple other existing business processes that are not directly relevant to security, but are either affected by security or provide data inputs into the security business processes. These include:

1. Regulatory compliance (legacy customs, immigration, border control, and financial oversight missions)
2. Economic development (trade, travel, and investment facilitation)
3. Border clearance (legacy customs and immigration missions)
4. Revenue collection (duties, tariffs, and taxes)

Breaking down the strategic framework into these six business functions can help to reveal synergies and commonalities in the global economic system. For example, in the area of risk assessment, there are literally dozens of projects in governments around the world and in the private sector that are focused on some variant of the "needle in the haystack" problem – trying to find a potential terrorist crossing a border checkpoint, or a cargo container containing a bomb, or an illicit financial transaction, amid the vast sea of people, goods, and data moving around the world. In each of these areas, it is possible to use subject-based queries or pattern-based predictive algorithms to focus inspection activities on high-risk people or things and associations of interest. System stakeholders can use this insight to find ways to create linkages between these diverse sets of activities.

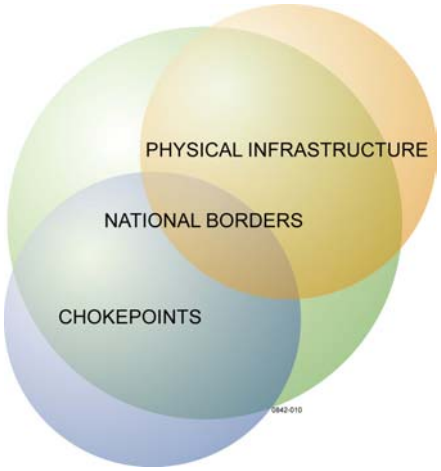
2. Control Points in the GMM Framework

A second key building block of a GMM framework is an assessment of the existing control points in the system. There are three key types of control points in the system (represented in **Chart II** below):

1. National borders
2. Movement chokepoints
3. Physical infrastructure

National borders exist as a means to enforce sovereignty. These are controlled both at formal checkpoints (either on the border or at internal points-of-entry, such as airport immigration stations) and to a lesser extent, along remote borders where attempts at smuggling or illegal immigration take place. Some countries, most notably the Schengen group within the European Union, have effectively removed their internal border controls to promote international movement and exchange among a core set of countries.

Chart II: GMM System Control Points



At the second level are chokepoints determined by the physical realities of movement and transport in the global economic system. These include key shipping bottlenecks such as the Panama and Suez Canals, the Straits of Bosporus, Gibraltar, Hormuz, and Malacca, and the mouths of the Mississippi and the Rhine rivers.

They include non-redundant transportation assets such as the Holland and Lincoln tunnels into Manhattan, the Ambassador Bridge and Detroit & Canada Tunnel connecting Detroit and Windsor, Ontario, the Jing Hu Freeway between

Shanghai and Beijing, or the Channel Tunnel between England and France. Other chokepoints include major payments and clearance systems such as key communications switches, or hub or root servers in the global information grid. Each of these chokepoints is a place that unmanaged and disparate activity must "pass through" if it is to be anything above localized activity. Because of this, they are both places of criticality (impairing the entire system if shut down) and places where certain types of security activities (e.g., inspection) can be effectively organized and conducted.

At the third level are a set of infrastructure-specific borders and control points such as fences and physical barriers to prevent entry into secure facilities. They also include passenger, baggage, and cargo screening systems for aviation and other modes of transportation as well as cybersecurity and information assurance activities for financial and communications systems.

At each of these three control point levels, there are existing security activities as well as new security activities that could be developed with minimal additional effort. It is also possible to integrate the three levels and prioritize security activities specific to certain flow types, locations, modes, and times.

3. Data Sources, Transactions and Information Flows in the GMM Framework

A third key building block of the GMM framework is the availability of existing data sources, transactions, and information flows in the global economy – all of the moving bits, bytes, signals and sentences coursing through the global economy. The ability to carry out the security business functions in the first section above in conjunction with the control points in the last section is dependent upon information about what is moving through the system – in both physical and transactional terms.

It is unrealistic to expect a system that provides perfect real-time information about what is moving through the system. Implementing such a vision for the system would be cost-prohibitive and likely to violate personal and commercial privacy norms. Instead, the framework should be built primarily upon data streams and information flows that exist today, many of which are imperfect and incomplete on their own, but collectively provide sufficient information about the near-real-time state of the system and its contents to facilitate and promote security.

Examples of such data sources include:[6]

People: Passenger name records (PNR) for commercial aviation. Visa and passport applications. Immigration declaration forms. Government and international watch lists. Pilot licenses. Commercial driver's licenses. Border crossing cards. Registered traveler program enrollments. Lost or stolen passport information.

Goods: Shipping manifest data. Customs declarations and clearances. Known shipper program enrollments. Container or pallet tags. Credit service bureau databases. Other supply chain messages and transactions (e.g., orders, invoices, shipment status, freight booking confirmations).

Conveyances: Maritime vessel registrations. Airplane registrations. Container or pallet tags.

[6] See also Markle Task Force Report, Protecting America's Freedom in the Information Age, Appendix H, "The Landscape of Available Information" for a fuller list of security-relevant data sources. Available at http://www.markletaskforce.org/documents/Markle_Full_Report.pdf

Money: Reporting requirements in many countries for large (ca. +$10,000) financial transactions. Counterfeiting monitoring systems.

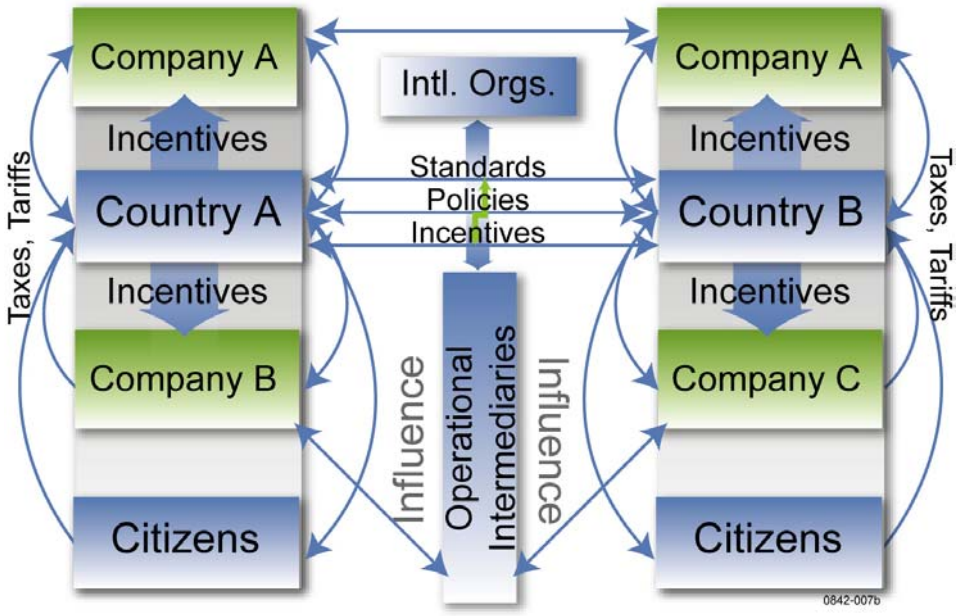
Information: Domain name registrations. Patent and trademark databases. Telephone directories. SIM Card purchases.

These data sources and information flows have security-relevant utility when used both on a stand-alone basis and (more importantly) in relation to one another. By mapping out the data sources that currently exist, it is possible to determine the existing or potential linkages between the different types of data, develop new information by integrating existing data streams, and locate any gaps in the system where new data might be required. It is also likely that commercial benefits can emerge from this process: key public and private stakeholders can find new ways to increase their overall efficiency. Further, by having a completed and integrated picture of these information flows, it is possible to build privacy and data protection into the system, and prevent misuse and unwarranted dissemination of personal information, by controlling access, using immutable audits, and anonymizing sensitive data as it moves through the system.

4. Stakeholder Relationships in the GMM Framework

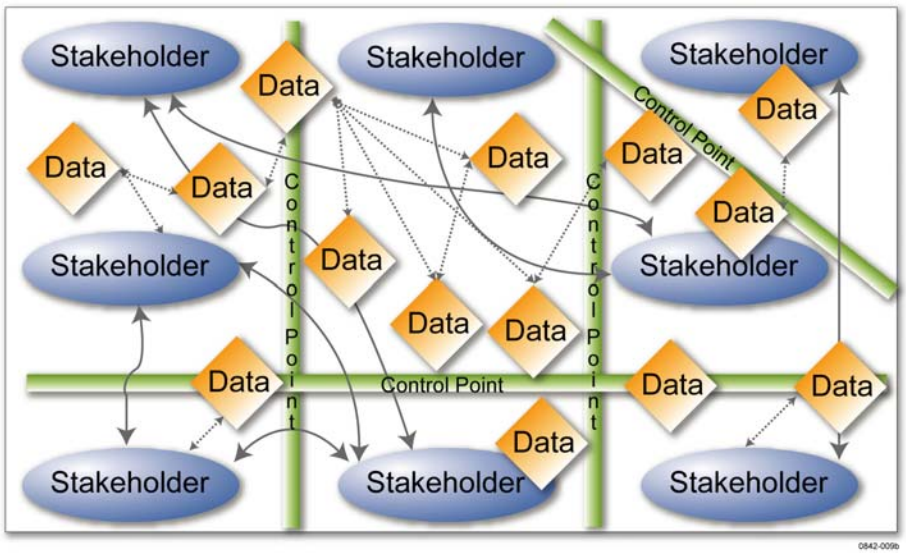
The fourth key building block of the GMM framework is the existing set of relationships among stakeholders in the system – governments (both national and sub-national), private sector companies of many types (e.g., shippers, manufacturers, banks, airlines, telecoms, retailers, service providers), international organizations (e.g., International Maritime Organization (IMO), International Civil Aviation Organization (ICAO), World Customs Organization (WCO), Interpol), public interest groups (including privacy and civil liberties advocates), and individuals. These stakeholders interact with one another in a complex and disorderly framework, and many of their interactions are tacit rather than formal. Some stakeholders are primarily facilitators and intermediaries, whereas others have responsibility more operational in nature. By mapping out the relationships among these various stakeholders, and understanding where interests converge and diverge, we can anticipate many of the obstacles that must be overcome to adopt an integrated strategy, and then use existing strong relationships to support the development of the framework. We can also start to envision a more orderly framework of stakeholder relationships, one in which relevant information is shared through standardized processes across the entire global economic system. **Chart III** on the next page provides a generic top-level map of these stakeholder relationships.

Chart III: GMM Stakeholder Relationships



These four building blocks – business functions, control points, data sources, and stakeholder relationships – provide the common template, the mesh canvas, upon which it is possible to build an integrated Global Movement Management framework. They make it possible to envision and develop a true "system-of-systems" for GMM. An overall understanding of these four building blocks and their interactions makes it possible to integrate dispersed security activities, and ensures that far-flung and unconnected activities can be potentially woven together and integrated as the system evolves. **Chart IV** below provides a representation of these last three building blocks and their interactions.

Chart IV: Interactions Among System Control Points, Data Sources, And Stakeholder Relationships



By going through the process of identifying and mapping these control points, data sources, and stakeholder relationships in the system (or in a single part of it), and integrating this analysis with a view of the key security activities in the **Chart I** business function framework, we can develop a clearer understanding of the challenges of security and resilience within the broader system or a component part of it.

The integrated Global Movement Management framework includes two elements, both of which are necessary to meet the key challenges, integrate security and resilience into the system, build new capabilities where needed, and translate this theoretical common picture into an operational reality. These are a governance structure and system architecture for GMM.

V. Governance Of Global Movement Management

The governance structure for Global Movement Management includes the set of relationships, rules, standards, policies, incentives, and penalties among system stakeholders that are necessary to develop and manage the system. A key reason why security and resilience have not been embedded into the global economic system since 2001 is the lack of an effective and responsive governance structure. Building cooperation and interconnectedness among GMM stakeholders is not easy, but it is critical to the development of the system. This section of the report discusses options and models for governance in Global Movement Management.

The form of any governance system must follow its basic function. The functions of the governance system for GMM are numerous and diverse, but come together to achieve a common outcome of system efficiency and operability. As such, the form of governance for GMM needs to be evolutionary and adaptable, using existing models and mechanisms but also developing new mechanisms that can achieve new outcomes for the system.

Given the nature and realities of the global economic system, the governance framework for Global Movement Management needs ultimately to have the following general characteristics:

1. **Distributed and decentralized:** The diverse nature of the system creates the need for power and decision-making need to be shared among all key system stakeholders, not localized in a single country or company. The structure should ideally resemble that used to govern "open source" software development, where stakeholders collaborate across borders, and key decisions are arbitrated openly and based on merit.

2. **Standardized and federated:** At first impression, this seems contradictory to the characteristics above. But it is possible to develop a system that is both decentralized and operates according to a common set of rules, standards, and interfaces, similar to the Internet. This contradiction can be solved through the proper sequencing of activities (agreeing upon standards in a decentralized process, but then enforcing their use once adopted).

3. **Incentive-driven:** The critical governance challenge for GMM is motivating system adoption. Many parts of the governance framework will be inherently voluntary, and it is necessary to find non-mandated ways to align the interests and resources of those who are concerned about threats to the system with those who have the ability to make investments in it. Private sector companies often resist making security-related investments unless they offer a demonstrable benefit (i.e., high-value threat protection, lower insurance rates) or a financial return unrelated to their security value (i.e., loss prevention, decreased logistics costs). Developing nations or nations perceiving themselves as low-risk are in many cases

unlikely to invest in security for similar reasons. Both of these funding imbalances can be overcome through the appropriate use of incentives. Also, liability issues are often a make-or-break concern when security-related investments are considered.

4. **Adaptive:** Able to change in response to new system imperatives and threats, and the introduction of new stakeholders.

There are a number of governance systems already in existence that can be building blocks for GMM governance and/or provide appropriate analogies for future governance activities. These include:

- Traditional general or domain-specific international organizations (e.g., UN, International Civil Aviation Organization, International Maritime Organization, World Customs Organization)
- International law enforcement organizations (e.g., Interpol, Europol, Financial Action Task Force)
- Negotiated treaties and agreements (e.g., Law of the Sea, Nuclear Non-Proliferation Treaty)
- National laws, mandates, or programs as *de facto* global standards (e.g., C-TPAT, Advanced Manifest Rule)
- Formal groups of nations (e.g., G8, OECD, APEC)
- Joint intergovernmental ventures (e.g., Space Station, high-energy particle physics)
- Open non-governmental collaborative networks for technology development and adoption (e.g., Linux, Apache, XML)
- Multinational business alliances and consortia (e.g., Bluetooth, W3C)
- Regulation-driven business oversight and compliance (e.g., GAAP, IAS, Sarbanes-Oxley)

A governance structure for GMM can be designed using, in part, proven approaches borrowed from many of these organizational types. Such approaches should not be applied uniformly across the system – instead, options should be considered based upon the characteristics of activity in individual parts of the system, broken out by business function and flow or mode.

Key questions to ask when considering a governance structure for a part of the system include:

1. Who has the domain knowledge and relevant expertise in this area?
2. Who has the legal, political, and operational control over the domain?
3. Are there potential non-security externalities, such as commercial benefits, from investments in security and resilience in this area?
4. Are the key stakeholders in this part of the system relatively homogenous or heterogeneous? Are they many or few?
5. Do existing stakeholders operate largely in an informal, trust-based environment, or are their relationships with each other very formal and legalistic?
6. Are there legacy governance activities in this part of the system that can be used as a foundation?

By answering these questions for a particular part of the system – e.g., financial transaction tracking, cargo certification, or immigration enforcement – we can begin to think about appropriate governance models for that part of the system. In many cases, it will be appropriate

to have distinctions within the model for the various stages of the system, including system development, rules-setting, and operations.

Take cargo tracking as an example. Shipping and transportation is almost exclusively a private sector activity on a global basis, with the exception of some defense and security-related shipping activities. It is quite likely that dual-use commercial benefits would be created by the development of security-driven investments in tracking capabilities, making it easier for companies to plan activities, monitor inventory, prevent theft, and reroute goods in-transit in response to shifts in demand or other external forces. There are millions of stakeholders in the system, of many different types, large and small, with diverse and competing interests – but a common interest in system efficiency and performance. Parts of the system have been traditionally very informal and trust-based, but the system has become increasingly formal in response to volume, automation, and new security requirements. A number of existing governance activities are relevant to cargo tracking, including the IMO's International Ship and Port Facility Security Code (ISPS) and the industry-driven consortium EPCglobal.

Given these current realities, it is possible to envision a governance model for cargo tracking where the private sector is motivated to fund security-related investments due to the potential dual-use commercial benefits of these investments, and the public sector is shaping the conditions that allow them to make these investments: leveling the playing field by creating alignment on standards, providing liability protection where necessary, and ensuring privacy and protection of commercially-sensitive data. **Chart V** provides additional detail on key parameters for governance within the cargo tracking example:

Chart V: Governance Model Characteristics: Cargo Tracking Example

Governance System Attributes	Development	Rules-Setting	Operations
Key System Actors	Private sector: through collaborative networks and consortia	Private and public sector together, via organizations like IMO	Private sector with thin government layer for security applications
Government Role	Facilitate standards-setting activity; limited funds for R&D if needed; consider political risk reduction measures	Ensure privacy, handle liability issues	Interface for security applications with law enforcement
Private Sector Role	Develop system with own funds	Play lead role in setting rules through an open and collaborative process	Operate the system
Degree of Centralization	Pure R&D can be decentralized, but strong imperative for development of common standards	Relatively centralized process	Decentralized
Level of Formality	Moderate level of formality	High level of formality	Moderate level of formality
Degree of Heterogeneity in this Portion of System	Consider multiple approaches in development of system	Single set of outcome-based rules with flexibility on means desired	Multiple approaches within parameters that ensure desired interoperability
Performance Metrics	e.g., Investment in system development relative to value of trade flow	e.g., Weighted percentage of countries and companies participating	e.g., Standard measures of cost, performance, effectiveness of security & resilience in system

Governance System Attributes	Development	Rules-Setting	Operations
Types of Incentives	Commercial externalities, liability protection, funded R&D	Reciprocity, transparency	Commercial externalities, green lanes, grants to developing countries, liability protection, reduced system risk, greater resiliency
Current Activities	EPCglobal, Operation Safe Commerce	ISPS	n/a

A similar thought process can be carried out for any other part of the system, using these six questions to determine what mix of relationships, rules, standards, policies, incentives and penalties that can motivate and enable the development of governance in that part of the system.

Incremental and evolutionary developments in multiple subcomponents (e.g., R&D, pilot projects, policy formation, standards-setting, public-private partnerships) can ultimately converge to form the *de facto* governance system for GMM. At some point it may become necessary to create an overarching governance structure that binds together these disparate parts of the system, but the potential near-term benefits of that comprehensive approach are outweighed by the likely delays and burdens of a top-down approach.

If the governance framework is developed in accordance with these parameters, the system will be more likely to overcome the four challenges highlighted earlier in **Section III**: integration of security and resilience with the commercial imperatives of the system; integrated of security and resilience with societal imperatives such as privacy and civil liberties; international cooperation and harmonization; and, cooperation between the public and private sector.

The integration of security and resilience with the commercial and societal imperatives of the system will be easier to achieve because private sector stakeholders and citizens groups will participate in the development of the governance framework for the system, and ensure that commercial imperatives and privacy and civil liberties interests are integrated from the start.

The need for both international cooperation and public-private sector cooperation will be addressed by more closely aligning the marginal costs and marginal benefits of security and resilience in the system through the use of incentives. Wealthy countries that have a direct incentive to improve security and resilience in developing countries will offer grants or loans to these countries to spur their investment. Critical private sector stakeholders will in certain cases be eligible for grants or other types of incentives that will ensure that investing in security is not a drain on profits, but aligned with improved long-run business performance.

VI. The GMM System Architecture

As discussed in **Section IV**, the global economic system is complex and heterogeneous – encompassing billions of interactions and transactions each day around the world. However, in spite of this complexity and heterogeneity, it is possible to break it down into its constituent security-relevant elements, and use these building blocks to create a holistic system architecture for GMM.

This system architecture has two key components. The first is general in nature: a way of thinking about Global Movement Management from a systems perspective, and a related set of

critical and overarching system requirements. The second part is a specific core system application, called the Global Movement Security Application (GMSA), which augments security and resilience in the global economy and leaves only a light footprint.

A. GMM System Requirements

An ideal Global Movement Management system would have a "Muhammad Ali" effect; it would "float like a butterfly," and not disrupt or degrade normal activity in the system, and then "sting like a bee," only manifesting itself after detecting anomalous or suspicious activities.

But such a system is likely to be impractical, at least in the near to medium term, for both cost and performance reasons. In the sprawling commotion of the global system there is no quick and easy way to identify an illicit flow, such as a potential terrorist or a suspicious cargo container. However, this system complexity and diversity can be turned from weakness into strength, through the process of identifying the elements of the existing system (as in **Section IV**, Building a GMM Framework) and applying a set of system requirements that can inform specific operational and technological choices related to Global Movement Management. The five most important requirements of a GMM system architecture are that it is **integrated, net-centric, layered, corrective, and risk-driven**.

The GMM system architecture needs to be **integrated** for three main reasons: to coordinate action, establish a common operational picture that creates new insights about potential threats, and share information across and among key system participants. If the GMM system architecture is not able to achieve these three goals, investments in the security and resilience of the system are likely to be wasted. It serves little purpose to develop a robust intelligence and risk analysis capability at a single port, or within a single mode of transportation, and not develop means to fuse that information to spot worrisome trends, and share it appropriately among critical stakeholders. Integration drives the need to create a service-oriented architecture that is loosely-coupled but uses common standards, common system platforms and interfaces, and/or middleware to bridge gaps between different systems.

Second, the system architecture needs to be **net-centric** in its design. The key imperatives of net-centric warfare – knowledge, speed, and precision – are also highly relevant to security and resilience activities in the global economic system, given its dispersed nature and the critical need for precise and real-time capabilities in many situations. This requirement creates the need to consider using a wide range of net-centric design principles and architectures.[7]
Third, the system architecture needs to be **layered** in recognition of the fact that no single defensive tool can ensure security, but that layered and redundant defenses can serve as a very effective means of prevention and deterrence to terrorist activities. As numerous experts on security and counter-terrorism have pointed out, if you have five independent layers that are "80% effective," you've created a system that is 99.97% effective, likely at a cost that is lower than creating one stand-alone "99.97% effective" tool.[8] This is a level of defense that is likely to deter terrorists from carrying out an attack against, or using, that element of the GMM system. The layered requirement drives the need for modular and federated architectures.

Fourth, the system architecture needs to be **corrective** – able to integrate human factors into any technology-driven solution, and give people the means to override warnings and correct false data that disrupt legitimate activities in the system. The passenger no-fly list in the United

[7] A thorough list can be found here: http://www.defenselink.mil/nii/org/cio/doc/NetCentric_Checklist_v2-1-3_May12.doc
[8] 1-((100%-80%)^5)=99.97%.

States today is an example of a system element where the capability for correction is lacking, and users are unable to easily remedy false information in the system. This is the direct result of using an insufficiently discerning metric such as someone's name, instead of a unique biometric identifier, for the no-fly list. This corrective requirement creates the need for data rectification tools, as well as auditing functions that prevent insider system misuse.

Finally, the system architecture needs to be **risk-driven**, allocating resources within the system in proportion to the potential severity and likelihood of the threat, the vulnerability of the particular asset or system, and the potential effectiveness of countermeasures within the system. This requirement creates the need to establish and track real-time performance metrics that can be used both for operational decision-making and for planning about future needs and requirements.

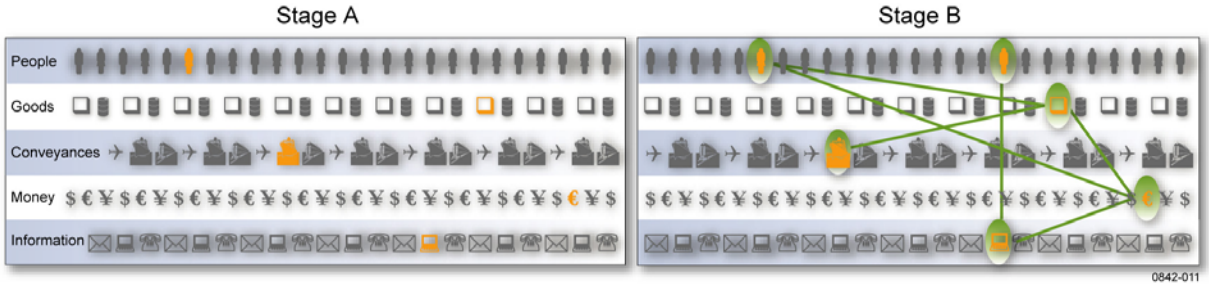
B. The Global Movement Security Application (GMSA)

Until now, this paper has not recommended a specific system, application, or project for Global Movement Management. GMM is first and foremost a way of looking at security and resilience in the global economy, and for the most part this paper draws back from proposing a single, unified vision for the system, instead suggesting that the appropriate system will naturally emerge if the right governance structures and system requirements are encouraged and established.

But this is true only up to a point. There is an urgent need to improve security and resilience in the global economic system, and this can only be accomplished through the addition of a new core set of tools and applications that can serve as the "brain" of the entire system.

Two key security imperatives for the system will be unfulfilled without this kind of intervention. First, it will be unable to integrate and analyze data across multiple flow types. Currently, within many flows it is possible to conduct risk management and targeting activities for people, or for containers, or for financial transactions. But it is difficult to conduct risk management in a way that is integrated across all of these flow types, and potentially reveal non-obvious information from such examinations. With such a capability, it is possible to move the analysis from Stage A to Stage B as depicted in **Chart VI**:

Chart VI: GMSA Risk Management Value Proposition



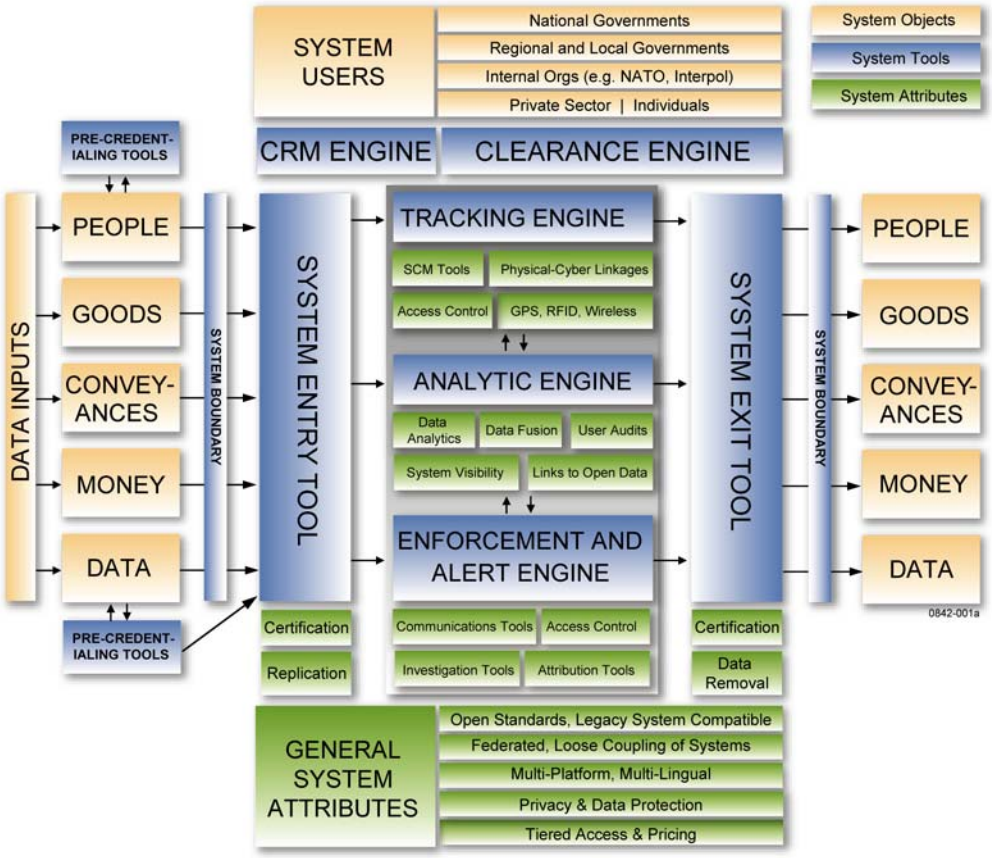
In Stage A of this chart, risky or suspected people, goods, conveyances, transactions, and communications are spotted but only analyzed in the context of risk management tools for that single flow type. Moving to Stage B, the relationships among risk information across the five flow types is analyzed, expanding the knowledge base about potential threats to the system.

Second, without a core system, the system will lack the ability to respond effectively and quickly to suspicious information or alerts moving through the system. The architecture below addresses both of these system gaps.

GMSA is intended to serve as the backbone for GMM security, as a core element of the broader "system of systems," supporting all of the other security and resilience activities that take place within the global economic system. Many elements of this "global utility" exist already in various legacy systems around the world – it would both interface with these systems and could provide new functionality where legacy systems do not provide the requisite level of security. It would work in a manner similar to a number of existing global utilities, such as the global financial clearing and settlement system, the International Telecommunications Union's payments system, and the four major airline computer reservation systems.

The system architecture for the GMSA concept is illustrated in **Chart VII** on the next page. The chart shows how GMSA fits conceptually into the broader Global Movement Management framework, as described in **Section IV** and the earlier parts of this chapter, and defines the core elements of the system.

Chart VII: GMSA System Architecture



Starting from the left-hand side of **Chart VII**, there are data inputs into the system, for each of the five key system flows (people, goods, conveyances, money, data) entering the system. They cross the system boundary – the point at which security activities are theoretically feasible (perhaps a national border, or the loading of a container, or the posting of a financial transaction) either with or without having been pre-credentialed and made a known entity to

the system. These **Pre-Credentialing Tools** can take multiple forms and involve a number of methods, such as applying for a passport or visa, or establishing a "known shipper" program.

These flows then interact with a **System Entry Tool** that is the gateway to the GMSA and the interface for the key functional and analytical tools of the system. The System Entry Tool registers the object in the system, certifies it in cases where pre-credentialing is relevant, and replicates and distributes the data inputs, based upon sets of established permissions, into further nodes in the system.

This data is then used by three distinct but interrelated "engines" in the system: a **Tracking Engine**, an **Analytic Engine**, and an **Enforcement and Alert Engine**. These three engines are essential to any GMM system, working together to deliver improved security and resilience to the system. Each is a distributed network of applications, running on tens of thousands of computers around the world, but interacting with each other to allow appropriate users a real-time picture of the parts of the system state that can inform security decisions.

The **Tracking Engine** is intended to monitor the progress of objects and flows within the system. It includes traditional supply chain management tools, and should be deeply integrated with existing commercially-relevant systems around the world. It allows users to see where objects are within the system and make decisions in response to changes in the environment, such as the shutdown of a key hub airport in Asia. The primary users of a Tracking Engine are commercial.

The Tracking Engine interacts with an **Analytic Engine** that uses all of the data that is aggregated across the system to detect system anomalies and provide government and law enforcement officials (who are its primary users) with the information that they need to protect the system. This Analytic Engine uses data analysis tools to find non-obvious relationships among the scattered billions of data points moving through the system. It protects privacy by anonymizing the identity of sensitive data moving through it. To prevent system misuse, it establishes immutable audits for user queries and for enforcement-related requests for additional (de-anonymized) information. This same data can be used to inform the users of the system about congestion, resources, availability of transport capacity, and other important issues that can support better decision-making and improve economic performance.

The information from the Analytic Engine is then the basis for activity in the **Enforcement and Alert Engine**, which can be used by law enforcement officials to communicate with key stakeholders in the system, closely monitor suspicious activity short of interdicting it, and where appropriate, take targeted steps to halt suspicious or illicit activity and trace its origins.

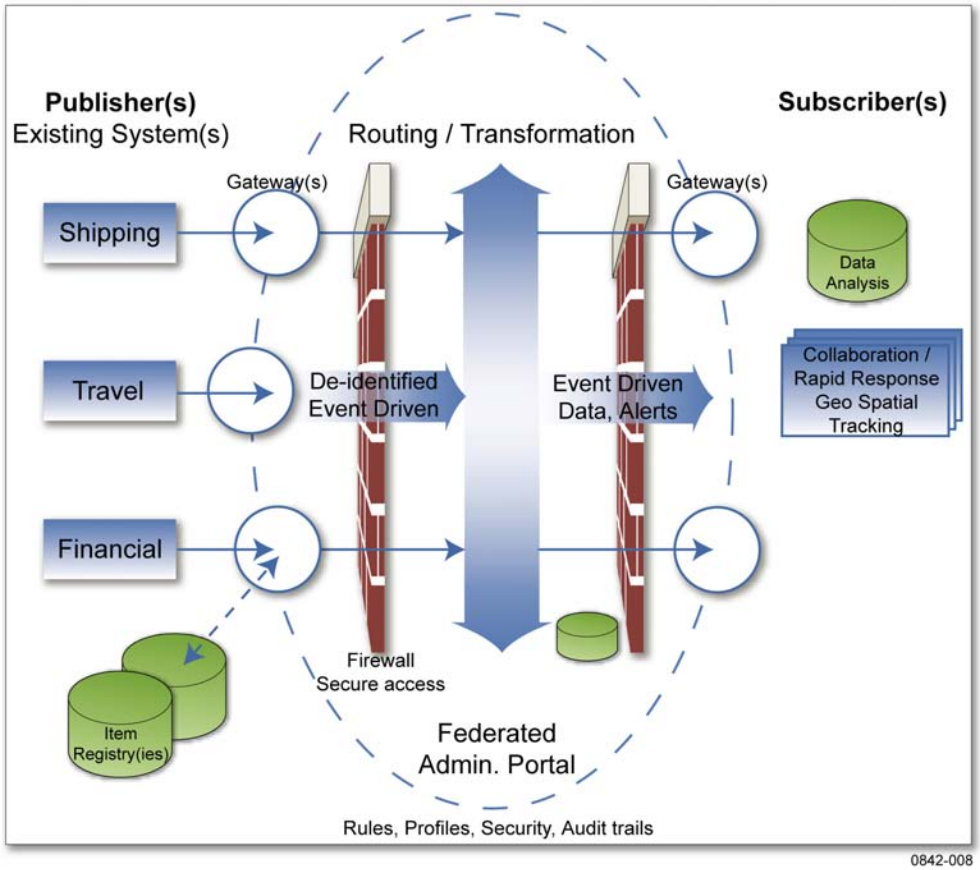
After an object has moved through the system and crossed outside of its boundaries (e.g., a person exiting an immigration station in their home country, or a package arriving on a truck at its destination), it then exits the system via a **System Exit Tool**, which certifies that the object is the same one that entered the system earlier, removes identifiable private data as appropriate, and archives other data where desired or required.

This system architecture:

- Takes a federated approach that leverages the capabilities of existing systems and processes and builds on them.
- Allows for and embraces open standards, including XML standards and industry specific vocabulary and identifiers, to allow more effective integration of these systems.
- Provides loose coupling of systems based on industry-accepted approaches and technologies such as Service Oriented Architecture to promote resiliency, flexibility and scalability. This approach avoids single points of vulnerability and enhances scalability by only routing required information.
- Places a high priority on privacy and data protection, using such tools as data anonymization, user authentication, immutable audits, and double-encrypted data, while enhancing the flow and quality of information shared. Only information required based on pre-defined events is "published" by the source systems and delivered to the authorized "subscribers" based on their requirements.
- Uses an iterative approach that allows participation at a measured pace while lowering risk for the participants.

A high level conceptual architectural diagram for the practical implementation of GMSA, based on these principles, is shown in **Chart VIII**:

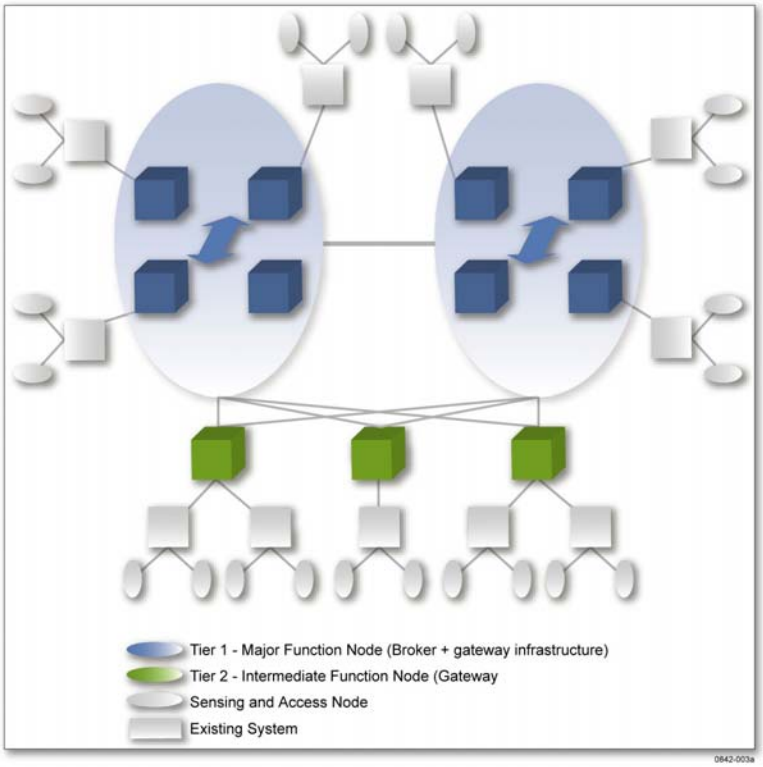
Chart VIII: GMSA System Architecture



This system architecture is related to healthcare surveillance systems in several ways, including similarities in its means of protecting privacy and personal data. Many envision that personal healthcare information can be aggregated and assessed, without compromising privacy, to create regional or national baseline profiles against which outbreaks, epidemics, and bioterror attacks can potentially be detected. In the same way, the GMSA can use aggregated and/or anonymized data to create risk management baseline profiles against which potential system threats and vulnerabilities can be detected and addressed.

Its implementation and enhancements can be iterative, moving outward from core nodes (created by earlier adopters of the system) to new points within the broader network, thereby lowering risk while enhancing system value to its many stakeholders. **Chart IX** depicts this iterative process and the relationship between the core and peripheral nodes in the system:

Chart IX: GMSA Iterative Functional Enhancement



The system architecture and approach places a strong focus on flexibility and adaptability. The system must be flexible enough to operate in a wide range of conditions – everything from high-tech operations centers to remote outposts in developing countries. It must be able to adapt in response to changes in the nature and severity of the threat, and changes in the resources and interests of system stakeholders.

This approach also allows the system to be set up in a way that provides tiered access and pricing capability, where the system (but not the data) may be leased as a service by companies or countries. This would align benefits with costs: wealthy countries that benefit the most from its adoption would bear the largest share of the costs, and developing nations can start

participating at an earlier stage than would otherwise be the case. If the cost burden is shared progressively, then these developing nations can participate and strengthen the value of the system to all stakeholders.

VII. Jumpstarting GMM: Near-Term Recommendations

The implementation of a Global Movement Management framework will be neither swift nor easy. But there are many things that policymakers and companies can do to hasten this process. Below are seven priority recommendations that would assist the implementation of Global Movement Management:

1. **Put GMM security on the agenda of key existing multilateral institutions and forums.** There have been many steps taken to develop security and resilience-related policies, international agreements, and standards in a number of international forums (e.g., G8, OECD, WTO, WCO, ICAO, IMO), but not in a way that is comprehensive and consistent with the GMM framework. In particular, the Secure and Facilitated International Travel Initiative (SAFTI) within the G8 might provide a good starting point for a broader international engagement on the question of security in the global economic system.

2. **Reorganize certain elements of national agencies consistent with the business function framework in this paper.** This functional approach to organizational structure and governance has been proposed by a number of leading academics practitioners, including the National Commission on the Public Service ("Volcker Commission") in the United States. For example, the U.S. Department of Homeland Security (DHS) is creating a new Screening Coordination and Operations (SCO) office inside of DHS responsible for assuring the consistency and quality of the application of screening technology across the Department. Similar changes might be warranted for other business functions (credentialing in particular) and in other countries. Reorganization should not be undertaken lightly, and is often an undesirable option due to the short-term pains of integration, but in certain cases the long-term benefits of rationalizing key operations outweigh these short-term difficulties.

3. **Encourage multilateral and national funding organizations to develop security benchmarks and funding mechanisms.** Multilateral organizations such as the World Bank, Asian Development Bank, and Inter-American Development Bank and national aid agencies such as USAID, CIDA, and DFID should consider new metrics to benchmark countries on security and should prioritize loan and grant activities to less-developed countries for basic GMM security capabilities such as electronic visa systems and customs automation. This can help to strengthen the weakest links in the system, many of which are likely to be otherwise targeted by terrorist groups as places to plan or originate their activities.

4. **Create a standing forum to resolve standards disputes.** There have been a number of protracted international disputes in the last few years, in areas such as biometric standards for passports. International organizations such as ICAO, IMO, and WCO have played a key role in developing these standards in their respective domains, but not enough attention has been paid to the linkages and interdependencies among related standards across the Global Movement Management system. A new limited-duration forum should be created, perhaps under the combined auspices of all of the groups noted above and working with technical organizations such as the ISO, to drive the adoption of high-level GMM-related security standards in critical areas where they are missing today.

5. **Create an independent standing forum to mediate on privacy and data protection issues as they pertain to the GMM system.** National differences on privacy and data protection issues are unlikely to be negotiated or compromised in the near term. But these honest disagreements can be mitigated if they are discussed openly, and if a new model of global reciprocity is developed for balancing security with privacy and data protection rights. This model could be developed by an international consortium of existing think tanks and research institutes, building off the work of groups such as the Markle Foundation, and working in coordination with international domain experts on privacy and inviting participation from the public and private sectors. A forum to discuss these issues can build trust and make it easier in the long run to implement challenging aspects of a GMM security and resilience strategy.

6. **Create a set of multinational pilot projects, with public sector and private sector participation, to test the core systemic and operational concepts of Global Movement Management.** These pilot projects should involve multiple flow types, operate across international boundaries, and be open to a wide and diverse set of participants. Lessons learned from these initial pilot projects, in addition to a longitudinal study of the relevant pilot projects that have been conducted in the recent past, can be used to refine the GMM concept and provide the agenda for the next stage of pilot and developmental activities.

7. **Develop mechanisms to conduct and test GMM security-related R&D on an international basis.** There are a number of specific areas in which investment in R&D has the potential to improve the effectiveness of security and resilience measures for the GMM system. Examples include radiological and nuclear detection technology, new means of biometric identification and authentication such as facial recognition, and privacy-enhancing anonymization and immutable audit technologies. There are certainly competitive reasons to keep R&D activities at the national level, especially if there are non-security applications for such technologies. However, these national benefits are often outweighed by the compelling need to develop breakthrough security technologies internationally, test them in cross-border pilot projects and testbeds, and promote their mass adoption on a global scale.

VIII. Conclusion: The GMM Imperative

Global Movement Management is not a vision of the perfect end-state for security in the global economic system. Instead, it is a process driven by a framework – a way of looking at the world and using certain insights to inform decisions about how to improve the security and resilience of the system. GMM is motivated today largely by the threat of terrorism – but with full awareness that threats and vulnerabilities change over time, and that all efforts must be undertaken in a way that preserves and protects the system's performance and core societal values. Given the vastness and complexity of the system, and the elusiveness of the threat, this is no easy task, and the ideas in this report are no panacea for challenges facing the global economic system. But if implemented thoughtfully and more widely over time, they can embed security and resilience into the system, protect it against threats known and unknown, and sustain global commerce and societal well-being in the years ahead.

For questions or comments about this white paper, please contact Scott Gould at w.scott.gould@us.ibm.com and Christian Beckner at cbeckner@us.ibm.com.

Acronyms

APEC	Asia-Pacific Economic Cooperation
ASI	America's Shield Initiative
CCI	Command, Control and Integration
CIDA	Canadian International Development Agency
CSI	Container Security Initiative
C-TPAT	Customs Trade Partnership against Terrorism
DFID	Department for International Development (UK)
DHS	Department of Homeland Security
EU	European Union
FAST	Free and Secure Trade
FATF	Financial Action Task Force
FinCEN	Financial Crimes Enforcement Network
FINTRAC	Financial Transactions Reports Analysis Centre
G8	Group of Eight
GAAP	Generally Accepted Accounting Principles
GMM	Global Movement Management
GMSA	Global Movement Security Application
GPS	Global Positioning System
IAS	International Accounting Standards
ICAO	International Civil Aviation Organization
IMO	International Maritime Organization
ISPS	International Ship and Port Facility Security Code
ISO	International Organization for Standardization
MRTD	Machine Readable Travel Document
NATO	North Atlantic Treaty Organization
OECD	Organization for Economic Co-operation and Development
OFAC	Office of Foreign Assets Control
PNR	Passenger Name Record
POE	Point-of-Entry/Point-of-Exit
RFID	Radio Frequency Identification
SAFTI	Secure and Facilitated International Travel Initiative
SCO	Screening Coordination and Operations
SENTRI	Secure Electronic Network for Traveler Rapid Inspection
SIM	Subscriber Identity Module
UN	United Nations
USAID	US Agency for International Development
US-VISIT	US Visitor and Immigrant Status Indicator Technology
W3C	World Wide Web Consortium
WCO	World Customs Organization
WMD	Weapons of Mass Destruction
WTO	World Trade Organization
XML	Extensible Markup Language

Key Works Consulted

Badolato, Ed. "Cargo Security: High-Tech Protection, High-Tech Threats." TR News, Nov/Dec. 2000.

Congressional Research Service. "Border and Transportation Security: The Complexity of the Challenge." Report # RL32839. March 29, 2005.

Congressional Research Service. "Border and Transportation Security: Selected Programs and Policies." Report # RL32840. March 29, 2005.

Congressional Research Service. "Border and Transportation Security: Possible New Directions and Policy Options." Report # RL3281. March 29, 2005.

European Commission. "Consultation Paper: Freight Transport Security." December 2003.

Flynn, Stephen. "Beyond Border Control." Foreign Affairs, Nov/Dec. 2000.

G8. "G-8 Secure and Facilitated International Travel Initiative (SAFTI)." Fact Sheet. June 2004.

Garvey, David. "Applications of Distributed, Networked Architectures to Port Security." From Securing the Port of New York and New Jersey, Network-Centric Operations Applied to the Campaign against Terrorism. Stevens Institute of Technology, 2004.

Jain, Rashmi and Michael Pennotti. "Assessment of Port Security in New York and New Jersey." From Securing the Port of New York and New Jersey, Network-Centric Operations Applied to the Campaign against Terrorism. Stevens Institute of Technology, 2004.

Kwek, Keng-Huat and Nandini Goswami. "Cost and Productivity Implications of Increased Security in Sea Trade Processes." The Logistics Institute – Asia-Pacific, 2004.

Lee, Hau L. and Michael Wolfe. "Supply Chain Security without Tears." Supply Chain Management Review, Jan/Feb. 2003.

Lee, Hau L. "Supply Chain Security: Are You Ready?" Stanford Global Supply Chain Management Forum. September 2004.

Lewis, Brian M., Alan L. Erera, and Chelsea C. White III. "Optimization Approaches for Efficient Container Security Operations at Transshipment Seaports." Paper at TRB 2003 Annual Meeting. November 2002.

Logistics Institute – Asia-Pacific. "Comparison of Singapore and USA Sea Cargo Container Export Processes." May 2003.

Loy, James and Robert Ross. "Global Trade: America's Achilles' Heel." Defense Horizons, National Defense University. February 2002.

Markle Foundation Task Force. "Creating a Trusted Network for Homeland Security." Second Report of the Markle Foundation Task Force. December 2003.

Morabito, Joseph. "Information Architecture to Counter Terrorist Threats to the Port of New York and New Jersey." From Securing the Port of New York and New Jersey, Network-Centric Operations Applied to the Campaign against Terrorism. Stevens Institute of Technology, 2004.

OECD. "Security in Maritime Transport: Risk Factors and Economic Impact." July 2003.

Perimeter Clearance Coalition. "The North American Perimeters: Advantages vs. Disadvantages." June 2003.

Rice, James B., Jr. and Federico Caniato. "Supply Chain Response to Terrorism: Creating Resilient and Secure Supply Chains" MIT Center for Transportation and Logistics Interim Report. August 8, 2003.

Sheffi, Yossi. "Supply Chain Management under the Threat of International Terrorism." International Journal of Logistics, 2001.

Sun, Shuang and John Yen. "Information Supply Chain: A Unified Framework for Information Sharing." In Proceedings of IEEE International Conference on Intelligence and Security Informatics (IEEE ISI-2005). Atlanta, GA, May 19-20, 2005.

Swedish Customs. "White Paper on Accreditation of Operators and Supply Chain Security." June 2003.

Webber, Joel. "Network-Centric Security for Canada-U.S. Supply Chains." Center for Strategic and International Studies and The Fraser Institute, 2005.

Willis, Henry H. and Davis S. Ortiz. "Evaluating the Security of the Global Containerized Supply Chain." RAND, 2004.

About the Global Leadership Initiative

IBM's Global Leadership Initiative (GLI) consists of former public sector executives, CEOs and leading academics who develop strategic thinking, relationships and opportunities for IBM Business Consulting Services Public Sector. GLI identifies critical public sector challenges, convenes expertise and develops thought leadership to address these stakeholders, and communicates its original ideas to key stakeholders through direct outreach and public discourse.

GLI supports the vision of BCS Public Sector – making a difference in peoples' lives by delivering innovative solutions for the world's greatest challenges. GLI partners with leading universities, international organizations, think tanks, and other public sector institutions in its pursuit of its mission. GLI interests cross a broad range of issue domains including security, governance, demographics, healthcare, economy, environment, education and energy.